UNIVERSITAS PRIMA INDONESIA

PROGRAM KOMPETISI KAMPUS MERDEKA 2023

BUKU PEMBELAJARAN DIGITAL SECURITY

Disusun Oleh:

Sigar P. Berutu
Rizki
Heriyanti
Tommy Leonard
Willy Tanjaya
Flora Nainggolan
Budi S.P. Nababan

Editor : Widodo Ramadhana

BUKU DIGITAL SECURITY

Penulis

Sigar P. Berutu

Rizki

Heriyanti

Tommy Leonard

Willy Tanjaya

Flora Nainggolan

Budi SP. Nababan

Editor

Widodo Ramadhana

ISBN

Penerbit

Unpri Press

KATA PENGANTAR

Salam sejahtera dan salam keamanan digital. Buku Digital Security dilatar belakangi adanya kebutuhan dan perkembangan teknologi dan informasi yang berkembang pesat di era society 5.0. Kebutuhan keamanan digital saat ini sangat penting mengingat banyaknya masalah hukum berkaitan dengan keamanan digital. Masyarakat sangat bergantung pada teknologi digital di semua aspek kehidupan sehingga diperlukan upaya memberikan pemahaman yang komprehensif guna mendukung peningkatan kompetensi mahasiswa dalam keamanan digital.

Buku ini memberikan pemahaman pentingnya menjaga keamanan dalam dunia digital yang penuh tantangan saat ini.

Ketika terhubung dan bergantung pada teknologi digital dalam aspek kehidupan sangat beresiko data yang dimililki oleh individu, masyarakat rentan beresiko menghadapi masalah yang berkaitan dengan ketidakamanan data. Buku ini akan membantu Anda memahami konsep dasar keamanan digital, mengidentifikasi potensi ancaman, dan memahami strategi serta praktik terbaik untuk melindungi diri sendiri dan aset digital.

Kami mengucapkan terima kasih kepada Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi yang telah memberikan bantuan pendanaan untuk menyelesaikan Buku mata kuliah Digital Security. Dan kami juga ingin mengucapkan terima kasih kepada semua yang telah berkontribusi dalam pembuatan Buku ini, termasuk para ahli keamanan digital, praktisi, dan peneliti yang telah berbagi

pengetahuan dan pengalaman mereka. Buku ini juga dapat diterapkan dalam berbagai konteks, baik untuk individu, bisnis, atau organisasi yang mencari cara untuk meningkatkan keamanan digital. Kami berharap Buku ini akan membantu memahami dan menjadi lebih sadar tentang tantangan keamanan digital yang ada, serta memberikan wawasan yang berguna untuk melindungi diri sendiri dan mengambil tindakan yang tepat guna menghadapi ancaman tersebut. Semakin banyak individu yang sadar akan pentingnya keamanan digital, semakin kuat perlindungan secara keseluruhan terhadap dunia maya.

Semoga Buku ini memberikan manfaat guna mendukung proses pembelajaran mata kuliah digital security di lingkungan pendidikan.

Salam hangat,

Tim Penyusun

DAFTAR ISI

PENDAHULUAN

A. LATAR BELAKANG

Era digital telah membawa kemajuan teknologi yang pesat, termasuk internet, komputasi awan, Internet of Things (IoT), dan komunikasi online. Hal ini mengakibatkan peningkatan penggunaan teknologi digital dalam berbagai aspek kehidupan, termasuk bisnis, pemerintahan, pendidikan, dan hiburan. Seiring dengan pertumbuhan teknologi digital, ancaman keamanan siber juga telah berkembang. Serangan siber seperti peretasan, pencurian data, serangan malware, dan phising menjadi lebih sering dan canggih. Organisasi dan individu semakin rentan terhadap kerugian finansial, pencurian identitas, dan pelanggaran privasi.

Semakin banyaknya data yang dikumpulkan dan disimpan secara digital memunculkan perhatian yang lebih besar tentang perlindungan data pribadi dan privasi individu. Undang-undang perlindungan data seperti GDPR di Uni Eropa dan berbagai undang-undang serupa di seluruh dunia menjadi penting dalam mengatur cara data pribadi dikelola dan dilindungi. Dalam konteks ini, hukum yang mengatur aspek-aspek keamanan digital, perlindungan data, dan privasi menjadi semakin kompleks dan berubah-ubah. Mahasiswa dan profesional dalam berbagai bidang, termasuk hukum, teknologi informasi, dan keamanan siber, perlu memahami kerangka hukum yang berkembang ini. Karena sifat global dari internet dan teknologi digital, matakuliah "Digital Security" juga mempertimbangkan dampak lintas batas hukum dalam lingkupnya. Pengaruh peraturan di satu negara dapat meluas ke negara lain, dan ini memerlukan

pemahaman yang mendalam tentang hukum internasional yang berkaitan dengan keamanan digital.

Dengan latar belakang ini, matakuliah "Digital Security" memberikan landasan penting bagi mahasiswa dan profesional untuk memahami dan menghadapi tantangan yang berkaitan dengan keamanan digital, perlindungan data, dan aspek hukum yang relevan dalam dunia yang semakin terhubung secara digital. Pemahaman tentang hukum ini penting untuk menjaga keamanan dan privasi dalam lingkungan digital yang terus berubah.

B. DESKRIPSI SINGKAT

"Digital Security" adalah matakuliah yang mempelajari kerangka hukum yang mengatur keamanan digital, perlindungan data, dan privasi dalam lingkungan teknologi informasi. Matakuliah ini membahas undang-undang dan peraturan terkait dengan perlindungan data pribadi, hukum kejahatan siber, insiden keamanan siber, dan tanggung jawab organisasi dalam menjaga keamanan sistem dan data. Mahasiswa akan memahami aspek hukum yang relevan dalam melindungi informasi digital, menghadapi ancaman siber, dan menjaga privasi individu dalam dunia yang semakin terhubung secara digital."

C. MATERI POKOK

Materi pokok matakuliah "Digital Security" berdasarkan tujuan pembelajaran mencakup topik-topik berikut:

1. Kerangka Hukum Keamanan Digital

- Pengenalan kepada kerangka hukum yang mengatur keamanan digital, termasuk peraturan nasional dan internasional yang relevan.

- Undang-undang perlindungan data pribadi, hak privasi, dan aspek hukum lain yang berkaitan dengan keamanan digital.

2. Ancaman Keamanan Siber

- Pemahaman tentang jenis-jenis ancaman keamanan siber, seperti peretasan, malware, serangan phishing, dan serangan DDoS (Distributed Denial of Service).
- Analisis dampak dari serangan keamanan siber pada organisasi atau individu, termasuk konsekuensi hukum yang mungkin timbul.

3. Proses Penegakan Hukum Digital

- Penjelasan tentang bagaimana penegakan hukum beroperasi dalam kasus kejahatan siber, termasuk peran lembaga penegak hukum dan prosedur penyelidikan.
- Pengumpulan bukti digital, teknik investigasi, dan proses penuntutan dalam kasus kejahatan siber.

D. TUJUAN PEMBELAJARAN

Setelah mengikuti pembelajaran ini mahasiswa mampu:

1. Mahasiswa dapat memahami dan menjelaskan kerangka hukum yang mengatur keamanan digital, termasuk undang-undang, peraturan, dan konsep dasar yang terkait.
2. Mahasiswa mampu untuk mengidentifikasi dan menganalisis ancaman keamanan siber yang mungkin dihadapi oleh organisasi atau individu, serta memahami konsekuensi hukum dari serangan tersebut.

3. Mahasiswa dapat menerapkan prinsip-prinsip perlindungan data, hak privasi, dan etika dalam situasi nyata, termasuk pemrosesan data pribadi dan pengelolaan privasi pelanggan atau pengguna.
4. Mahasiswa dapat pemahaman tentang bagaimana proses penegakan hukum beroperasi dalam kasus kejahatan siber, termasuk tahapan penyelidikan, pengumpulan bukti, dan penuntutan.
5. Mahasiswa dapat mengidentifikasi dan memahami implikasi hukum terkait dengan keputusan bisnis dan teknologi, serta mengambil tindakan yang sesuai untuk mematuhi peraturan yang berlaku.

MATERI

I

KERANGKA HUKUM KEAMANAN DIGITAL

Indikator Keberhasilan

Setelah mempelajari Materi 1 tentang Kerangka Keamanan Digital ini indikator keberhasilan adalah apabila anda dapat:

- Mengidentifikasi Undang-Undang dan Peraturan Nasional yang relevan yang mengatur keamanan digital dan perlindungan data pribadi.
- Menguraikan implikasi hukum dari pelanggaran data pribadi dan pelanggaran keamanan siber, termasuk sanksi yang mungkin diterapkan.
- Mengaitkan Kasus Nyata Atau Skenario Dengan Aspek-Aspek Hukum Dalam Kerangka Keamanan Digital, Termasuk Hak Privasi Dan Perlindungan Data Pribadi.

A. KERANGKA HUKUM YANG MENGATUR KEAMANAN DIGITAL DAN KONSEP DASAR YANG TERKAIT

Kerangka hukum yang mengatur keamanan digital adalah seperangkat undang-undang, peraturan, dan kebijakan yang diciptakan untuk mengatur dan melindungi keamanan serta integritas informasi dalam lingkungan digital. Kerangka hukum ini memberikan panduan tentang apa yang diizinkan dan dilarang dalam konteks keamanan siber, perlindungan data pribadi, hak

privasi, serta tanggung jawab organisasi dan individu terkait dengan keamanan digital.

Kerangka hukum yang mengatur keamanan digital dapat mencakup berbagai aspek, termasuk:

1. Perlindungan Data Pribadi: Undang-undang perlindungan data pribadi mengatur cara data pribadi harus dikelola, diproses, dan dilindungi. Ini termasuk hak-hak individu terhadap data pribadi mereka dan kewajiban organisasi untuk menjaga kerahasiaan data tersebut.
2. Hukum Keamanan Siber: Hukum keamanan siber adalah bagian penting dari kerangka hukum yang mengatur tindakan yang melibatkan akses ilegal, peretasan, malware, serangan phishing, dan serangan siber lainnya. Hukum ini menentukan sanksi dan konsekuensi hukum bagi pelanggaran keamanan siber.
3. Hak Privasi: Hukum hak privasi melindungi hak individu terhadap privasi mereka dalam dunia digital. Ini termasuk regulasi yang membatasi pengumpulan, penggunaan, dan penyebaran informasi pribadi.
4. Hak Cipta dan Kekayaan Intelektual: Kerangka hukum ini mencakup hukum hak cipta yang mengatur hak-hak pemilik konten digital dan bagaimana hak ini harus dihormati dalam konteks digital.
5. Hukum Kontrak Elektronik: Hukum kontrak elektronik mengatur validitas dan penegakan kontrak yang dibuat secara elektronik, termasuk pembelian online dan transaksi bisnis digital.
6. Hukum Komunikasi Elektronik: Hukum ini mengatur komunikasi elektronik, seperti surat elektronik dan komunikasi melalui platform

pesan instan, serta hak dan kewajiban dalam konteks komunikasi digital.

Kerangka hukum yang mengatur keamanan digital berfokus pada perlindungan kepentingan individu dan organisasi dalam lingkungan digital yang semakin kompleks. Melalui kerangka hukum ini, aturan dan peraturan ditetapkan untuk menjaga keamanan data, melindungi hak privasi, dan memfasilitasi penggunaan teknologi digital dengan cara yang sah dan etis. Organisasi dan individu harus memahami dan mematuhi kerangka hukum ini untuk menghindari potensi sanksi hukum dan menjaga integritas dan keamanan informasi dalam era digital.

Berikut adalah peraturan nasional dan internasional yang relevan dalam kerangka hukum yang mengatur keamanan digital:

1. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 (UU ITE).
2. Peraturan Pemerintah Nomor 80 Tahun 2019 tentang Perdagangan ... nasional dan internasional, melalui ekonomi digital.
3. Perlindungan Hak Asasi Digital.
4. Undang-undang Nomor 35 Tahun 2014 tentang Perubahan Undang-Undang No 23 Tahun 2002 tentang Perlindungan Anak.
5. Personal Data Privacy Ordinance of 1995 (PDPO) di Hong Kong sebagai peraturan perundang-undangan nasional pertama yang mengatur masalah privasi dan data diri.

6. Peraturan Perpustakaan Nasional Republik Indonesia Nomor 5 Tahun 2022 tentang Layanan Angka Standar Buku Internasional (International Standard Book Number)

Peraturan pemerintah Indonesia mengatur keamanan data pribadi melalui berbagai undang-undang dan peraturan, dengan fokus utama pada Perlindungan Data Pribadi. Undang-undang yang mengatur aspek ini adalah Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang memiliki Amandemen pada tahun 2016 dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas UU ITE. Dalam undang-undang ini, terdapat ketentuan yang menjelaskan hak dan kewajiban terkait data pribadi, perlindungan privasi, serta sanksi atas pelanggaran data pribadi.

Selain itu, pemerintah Indonesia juga memiliki peraturan lain yang lebih khusus terkait dengan perlindungan data pribadi, yaitu Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Pelaksanaan UU ITE. Peraturan ini mengatur lebih rinci tentang data pribadi, termasuk ketentuan-ketentuan untuk pemrosesan data pribadi, hak individu terhadap data pribadi mereka, dan kewajiban pemilik data pribadi untuk melindungi dan menjaga kerahasiaan data tersebut.

Selain itu, Badan Perserikatan Bangsa-Bangsa telah mengeluarkan Pedoman Perlindungan Data Pribadi Global yang mendorong praktik pengelolaan data pribadi yang aman dan etis. Penting untuk diingat bahwa peraturan-peraturan ini terus berkembang sesuai dengan perkembangan teknologi dan kebutuhan perlindungan data pribadi. Oleh karena itu,

organisasi dan individu di Indonesia harus memahami dan mematuhi peraturan tersebut untuk menjaga keamanan dan privasi data pribadi serta untuk menghindari potensi sanksi hukum.

Konsep dasar dalam keamanan digital adalah prinsip-prinsip yang mendasari pemahaman tentang bagaimana melindungi sistem dan data dalam lingkungan digital yang rentan terhadap ancaman keamanan siber. Kerentanan, ancaman, dan risiko adalah unsur-unsur kunci yang perlu dipahami dalam konteks ini. Kerentanan merujuk pada potensi celah atau kelemahan dalam sistem yang bisa dimanfaatkan oleh pihak yang tidak sah. Ancaman mencakup berbagai serangan seperti peretasan, malware, dan serangan phishing yang dapat merusak sistem atau mencuri data. Sementara risiko adalah hasil dari ancaman dan kerentanan yang mungkin menyebabkan kerugian atau kerusakan.

Prinsip-prinsip pengamanan digital melibatkan pemahaman tentang prinsip-prinsip pertahanan dalam kedalaman (defense in depth) di mana lapisan-lapisan keamanan diterapkan untuk mengurangi risiko. Prinsip kebutuhan terhadap prinsip paling sedikit (principle of least privilege) adalah prinsip lain yang mengatur akses terhadap data dan sistem. Selain itu, konsep keamanan data, pemantauan dan respons keamanan (*security monitoring and incident response*), serta prinsip privasi by design adalah bagian penting dari konsep dasar dalam keamanan digital.

Memahami konsep dasar ini penting dalam merancang, mengimplementasikan, dan menjaga keamanan dalam dunia digital yang terus berkembang. Dengan pemahaman yang kuat tentang kerentanan,

ancaman, risiko, serta prinsip-prinsip keamanan, organisasi dan individu dapat mengambil langkah-langkah yang lebih efektif dalam melindungi data dan sistem mereka dari ancaman keamanan siber.

Konsep dasar dalam keamanan digital meliputi:

1. Kerahasiaan: Konsep pertama dari keamanan digital adalah kerahasiaan. Maksudnya di sini adalah sistem tersebut membatasi akses dan hanya dapat diakses oleh orang yang berwenang. Hal ini bertujuan untuk menjaga kerahasiaan data dan informasi yang disimpan dalam sistem digital
2. Integritas: Konsep kedua dalam keamanan digital adalah integritas. Integritas dimaksudkan untuk penyampaian informasi yang benar, tepat serta akurat kepada publik. Perusahaan wajib menjaga informasi yang ada, agar data tersebut tidak bocor kepada pihak yang tidak berkepentingan. Integritas ini bisa dalam bentuk enkripsi seperti tanda tangan digital atau certificate authority (CA)
3. Ketersediaan: Konsep ketersediaan dalam keamanan digital adalah totalitas dari perusahaan, sehingga tidak ada kendala dalam hal transaksi atau yang lainnya. Hal ini bertujuan agar pelanggan tidak kecewa dengan sistem yang ada dan tidak berpindah ke kompetitor yang lain.
4. Perlindungan Hak Asasi Digital: Hak asasi digital merupakan salah satu bentuk hak asasi manusia universal yang bersifat konkret dan dijamin oleh hukum internasional serta konstitusi negara-negara di dunia. Hak asasi digital dipahami sebagai sekumpulan hak-hak masyarakat untuk mengakses, menggunakan, menciptakan, menyebarluaskan kerja digital,

serta untuk mengakses dan menggunakan komputer dan perangkat elektronik lainnya, termasuk jaringan komunikasi, khususnya internet.

5. Kewarganegaraan Digital: Kewarganegaraan digital (digital citizenship) mengklasifikasikan sembilan elemen utama dalam tiga prinsip dasar, yaitu aman (safe), cerdas (savvy), dan sosial (social). Setiap tema/elemen meliputi tiga tingkat dukungan (aman, cerdas, dan sosial) yang bisa (atau harus) diajarkan segera setelah anak-anak kita pertama dapat mengambil perangkat dan mulai berinteraksi dengan itu. Pertama; keselamatan, berfokus pada melindungi diri sendiri dan melindungi orang lain, dan menciptakan dasar kewarganegaraan digital. Yang berikutnya adalah savvy yang berfokus pada konsep di sekitar mendidik diri sendiri dan berhubungan dengan orang lain. Konsep ini dibangun berdasarkan konsep keselamatan. Dan akhirnya, prinsip pedoman sosial berkomitmen untuk membantu setiap orang membuat keputusan mencontohkan komitmen kita untuk menghormati diri sendiri dan menghormati orang lain. Di sinilah kita sepenuhnya menyadari kemungkinan pengalaman online.

Lembar Kerja

Tabel 1. Matrik Diskusi Kerangka Hukum Yang Mengatur Keamanan Digital Dan Konsep Dasar Yang Terkait

No	Poin diskusi	Deskripsi
1	Undang-Undang Terkait	Diskusikan undang-undang yang mengatur keamanan digital di negara Anda dan bagaimana mereka memengaruhi organisasi dan individu.
2	Perlindungan Data	Jelaskan bagaimana undang-undang

	Pribadi	perlindungan data pribadi memengaruhi cara data pribadi dikelola dan dilindungi.
3	Konsep Dasar Keamanan Digital	Diskusikan konsep dasar keamanan digital seperti kerentanan, ancaman, dan risiko, serta bagaimana mereka berperan dalam keamanan siber.
4	Prinsip Pertahanan dalam Kedalaman	Bahas prinsip pertahanan dalam kedalaman (defense in depth) dan bagaimana lapisan-lapisan keamanan dapat mengurangi risiko keamanan digital.
5	Prinsip Kebutuhan Terhadap Prinsip Paling Sedikit	Jelaskan prinsip kebutuhan terhadap prinsip paling sedikit dan bagaimana prinsip ini membatasi akses ke data dan sistem.
6	Prinsip Etika dalam Pengelolaan Data	Diskusikan pentingnya prinsip etika dalam pengelolaan data dan bagaimana etika berperan dalam melindungi privasi individu.
7	Studi Kasus Pelanggaran Keamanan	Bagikan studi kasus pelanggaran keamanan digital yang terjadi dan analisis konsekuensi hukum yang timbul dari kasus tersebut.
8	Tindakan Pencegahan dan Kepatuhan	Diskusikan tindakan yang dapat diambil oleh organisasi untuk mencegah pelanggaran keamanan digital dan mematuhi peraturan hukum yang berlaku.

Format di atas hanya sebagai panduan diskusi saja, kelompok dapat memberikantambahan atau menyesuaikan sesuai kebutuhan;

Matriks diskusi ini dapat membantu mengarahkan percakapan tentang kerangka hukum dan konsep dasar dalam keamanan digital, serta bagaimana prinsip-prinsip ini memengaruhi praktik bisnis dan perlindungan data pribadi.

B. Implikasi Hukum Dari Pelanggaran Data Pribadi Dan Pelanggaran Keamanan Siber, Termasuk Sanksi Yang Mungkin Diterapkan

Implikasi hukum dari pelanggaran data pribadi dan pelanggaran keamanan siber memiliki dampak yang signifikan. Ketika data pribadi seseorang diretas atau diakses tanpa izin, atau saat sistem keamanan siber disusupi, undang-undang privasi dan keamanan siber berlaku. Pelanggaran data pribadi dapat mengakibatkan sanksi finansial yang substansial, tergantung pada tingkat pelanggaran dan yurisdiksi hukum yang berlaku. Selain itu, individu yang terdampak dapat menggugat pelaku pelanggaran secara perdata untuk mendapatkan ganti rugi atas kerugian yang mereka alami. Di sisi lain, dalam pelanggaran keamanan siber, undang-undang kejahatan siber dapat memberikan dasar hukum bagi penyelidikan dan penuntutan pidana terhadap pelaku, yang berpotensi menghadapi hukuman penjara. Pelaku juga dapat menghadapi tuntutan perdata dari pihak-pihak yang menderita kerugian, dan kerugian reputasi yang signifikan bagi entitas yang terkena dampak. Oleh karena itu, perlindungan data pribadi dan keamanan siber yang baik adalah penting, dan tindakan pencegahan harus diambil untuk menghindari implikasi hukum yang merugikan.

Kejahatan data pribadi adalah suatu tindakan yang melibatkan akses, penggunaan, atau pengungkapan data pribadi individu tanpa izin atau tanpa langkah-langkah yang memadai untuk melindungi informasi tersebut. Implikasi hukum dari pelanggaran data pribadi adalah serius. Ini mencakup pelanggaran terhadap undang-undang privasi yang berlaku, seperti Regulasi Perlindungan Data Umum (GDPR) di Uni Eropa atau Undang-Undang Privasi Konsumen California (CCPA) di Amerika Serikat. Sanksi yang mungkin diterapkan termasuk denda yang substansial yang dapat dikenakan oleh otoritas pengawas. Denda ini dapat mencapai jumlah yang sangat besar, tergantung pada tingkat pelanggaran dan wilayah hukum yang berlaku. Selain itu, individu yang terkena dampak pelanggaran data pribadi dapat menggugat pihak yang bertanggung jawab atas pelanggaran tersebut secara perdata untuk mendapatkan ganti rugi atas kerugian yang mereka alami. Dengan demikian, penting bagi organisasi dan entitas yang memproses data pribadi untuk mematuhi undang-undang privasi yang berlaku dan menjaga keamanan data dengan cermat untuk menghindari sanksi hukum dan kerugian finansial yang mungkin timbul akibat pelanggaran data pribadi.

Kejahatan keamanan siber adalah tindakan yang melibatkan upaya tidak sah untuk mengakses, merusak, atau mengganggu sistem komputer, jaringan, atau infrastruktur digital dengan tujuan mencuri data, mengganggu operasi, atau merusak integritas informasi. Implikasi hukum dari pelanggaran keamanan siber adalah serius, terutama dengan adanya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. UU ITE memberikan kerangka hukum yang mengatur tindakan kriminal dalam ranah keamanan siber, seperti hacking, pencurian data, dan serangan siber lainnya.

Pelaku pelanggaran keamanan siber di Indonesia dapat menghadapi sanksi pidana, termasuk hukuman penjara, serta sanksi perdata jika ada pihak yang menderita kerugian akibat tindakan tersebut. Selain itu, pelanggaran keamanan siber juga dapat merusak reputasi entitas yang terkena dampak, baik secara finansial maupun dalam hal citra dan kepercayaan pelanggan. Oleh karena itu, penting bagi organisasi dan individu untuk menjaga keamanan siber dengan cermat dan mematuhi undang-undang yang berlaku untuk menghindari konsekuensi hukum yang serius.

Ketentuan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia memiliki peran kunci dalam menangani pelanggaran keamanan siber. UU ITE mengatur berbagai aspek terkait keamanan siber, termasuk tindakan yang dianggap sebagai pelanggaran. Di bawah UU ITE, tindakan seperti hacking, pencurian data, penyebaran malware, dan serangan siber lainnya dianggap ilegal dan dapat mengakibatkan tindakan hukum. Pelaku pelanggaran keamanan siber di Indonesia dapat menghadapi sanksi pidana yang mencakup hukuman penjara dan denda. Hukuman ini bervariasi tergantung pada tingkat pelanggaran dan kerugian yang diakibatkan. Selain sanksi pidana, UU ITE juga memungkinkan tuntutan perdata oleh pihak yang menderita kerugian akibat pelanggaran tersebut. Oleh karena itu, ketentuan UU ITE memiliki peran penting dalam memberikan kerangka hukum yang jelas untuk menindak pelanggaran keamanan siber di Indonesia, dengan harapan bahwa hal ini akan mendissuasi pelaku pelanggaran dan memberikan perlindungan bagi korban pelanggaran keamanan siber.

Tabel 2. Perbadingan Kejahatan Data Pribadi dengan Kejahatan Keamanan Siber

Kriteria Perbedaan	Kejahatan Data Pribadi	Kejahatan Keamanan Siber
Definisi	Melibatkan akses, penggunaan, atau pengungkapan data pribadi tanpa izin atau perlindungan yang memadai.	Upaya tidak sah untuk mengakses, merusak, atau mengganggu sistem komputer atau jaringan dengan tujuan mencuri data, mengganggu operasi, atau merusak integritas informasi.
Fokus	Fokus pada data pribadi individu, seperti informasi pribadi, keuangan, atau medis.	Fokus pada keamanan sistemkomputer, jaringan, dan infrastruktur digital.
Regulasi Utama	Diatur oleh undang-undang perlindungan data pribadi, seperti GDPR (di Eropa) atau UU PDP (di Indonesia).	Diatur oleh Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan undang-undang yang berkaitan dengan keamanan siber.
Implikasi Hukum	Sanksi dapat mencakup denda yang substansial, baik dalambentuk sanksi administratif	Sanksi melibatkan hukuman pidana, termasuk hukuman penjara, dan sanksi perdata jika ada pihak

	maupun tuntutan hukumsipil.	yang menderita kerugian akibat tindakan tersebut.
Korban	Individu yang data pribadinya dilanggar, serta organisasi yang memproses data pribadi.	Organisasi yang menjadi sasaran serangan siber, seringkali dengan potensi kerugian finansial dan reputasi.
Perlindungan dan Pencegahan	Melibatkan perlindungan data pribadi, termasuk peraturan privasi, enkripsi, dan manajemen akses.	Melibatkan keamanan siber, seperti firewall, deteksi intrusi, dan pemantauan keamanan.
Penegakan Hukum	Dilakukan oleh otoritas pengawas perlindungan data pribadi dan tuntutan hukum sipil oleh individu yang terkena dampak.	Dilakukan oleh penegak hukum, dan Badan Siber dan Sandi Negara (BSSN) di Indonesia, dengan sanksi pidana dan perdata sebagai alat penegakan.

Tabel di atas mencantumkan perbedaan utama antara kejahatan data pribadi dan kejahatan keamanan siber dalam hal definisi, fokus, regulasi, implikasi hukum, korban, perlindungan, dan penegakan hukum. Ini membantu untuk

memahami perbedaan antara dua jenis pelanggaran ini dan betapa pentingnya untuk mematuhi regulasi dan menjaga keamanan data serta keamanan siber.

C. Studi Kasus: Keterkaitan Hukum, Keamanan Digital, dan Privasi Data dalam Dunia Nyata

1. Contoh Kasus

Di Indonesia kasus terbaru mengenai kebocoran data pribadi terjadi pada perusahaan ber plat merah yaitu PT PLN dan Indihome (Telkom), diduga PT PLN telah membocorkan 17 Juta data pribadi konsumenya yang di paparkan oleh seorang hacker di media social miliknya, Pelaku menawarkan beberapa jenis data pelanggan, seperti ID lapangan, ID pelanggan, nama konsumen, alamat, tipe energi, nomor meter, dan besaran KWh. Susul PLN, 26 Juta data pribadi konsumen Indihome telah bocor dan diperjual belikan di forum hacker. Akibat pembobolan data pribadi Konsumen di PT PLN timbul pertanyaan mengenai keamanan data pribadi konsumen yang sudah terkumpul apakah data pribadi konsumen yang sudah terkumpul benar-benar dalam posisi yang aman atau data pribadi tersebut berada dalam posisi yang rentan untuk diretas.

2. Aspek Hukum yang terkait

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, yang telah disahkan oleh Presiden Republik Indonesia, Jokowi, pada tanggal 17 Oktober 2022, memiliki tujuan utama untuk melindungi data pribadi yang dikelola oleh penyelenggara sistem elektronik (PSE) dan mencegah penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab. Keberadaan undang-undang ini memberikan perhatian khusus terhadap isu-isu terkait kebocoran data dan mendorong pencarian solusi yang jelas dan aman. Hal ini penting mengingat perkembangan terus menerus dalam teknologi dan internet, yang selalu menyertai potensi kejahatan siber. Kejahatan siber

memiliki dampak yang meluas, mencakup individu, kelompok, dan bahkan dapat membahayakan keamanan nasional, serta menimbulkan kerugian ekonomi, perbankan, politik, dan berbagai aspek kehidupan masyarakat. Oleh karena itu, perlindungan data pribadi dan keamanan siber menjadi hal yang sangat penting dalam menghadapi tantangan di era digital ini.

Dengan pengesahan undang-undang perlindungan data pribadi ini, diharapkan akan memberikan penyelesaian terhadap masalah kebocoran data pribadi yang sering terjadi di Indonesia. Undang-Undang Perlindungan Data Pribadi ini dirancang dengan tujuan utama menjaga konsep hak privasi individu. Dalam naskah akademiknya, undang-undang ini menekankan bahwa "hak privasi melalui perlindungan data pribadi merupakan elemen kunci bagi kebebasan dan harga diri individu." Oleh karena itu, tujuan dari pengesahan regulasi perlindungan data pribadi ini adalah untuk melindungi kepentingan konsumen dari penyalahgunaan data pribadi mereka.

Dari analisis di atas, pengesahan undang-undang perlindungan data pribadi ini dapat dianggap sebagai solusi bagi permasalahan kebocoran data pribadi yang sering terjadi saat ini. Selain itu, dengan undang-undang ini, masyarakat Indonesia akan mendapatkan kepastian hukum. Meskipun Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen juga ada, hak yang paling relevan dengan isu kebocoran data adalah hak kelima yang menyatakan, "Hak untuk mendapat advokasi, perlindungan, dan upaya penyelesaian sengketa perlindungan konsumen secara patut."

3. Implikasi Hukum

Jika terjadi kebocoran data pribadi yang dikelola oleh suatu perusahaan, maka perusahaan tersebut bertanggung jawab atas insiden tersebut, baik itu disebabkan oleh peretasan pihak ketiga maupun sengaja dibocorkan. Perusahaan e-commerce, sebagai badan hukum korporasi, diperlakukan sebagai pengendali data pribadi dan tunduk pada peraturan perlindungan data pribadi yang diatur dalam Undang-Undang Perlindungan Data Pribadi.

Transaksi jual beli secara online atau pemindahan kepemilikan dari penjual kepada konsumen harus melibatkan sebuah akad. Walaupun e-commerce dilakukan secara daring tanpa pertemuan langsung, perjanjian tetap diatur dalam bentuk elektronik. Setelah kita memasukkan data pribadi ke dalam aplikasi e-commerce, biasanya aplikasi belanja online akan menampilkan kontrak antara pengguna atau konsumen dengan toko online tersebut di situs web. Kontrak ini dapat disusun oleh toko online itu sendiri atau dinyatakan secara sepihak. Sebagai pengguna, kita hanya perlu mencentang kolom persetujuan apakah kita menyetujui perjanjian yang tercantum atau tidak. Oleh karena itu, kita tidak berperan dalam menyusun perjanjian tersebut. Inilah yang dapat dianggap sebagai risiko ketika mendaftarkan diri kita secara daring. Jika kita tidak membaca perjanjiannya dengan cermat, hal ini bisa menjadi bumerang bagi kita sendiri. Sudaryatmo menjelaskan bahwa perjanjian elektronik sering kali bersifat klausal baku, di mana perjanjian tersebut dibuat secara sepihak oleh pihak yang memiliki posisi yang lebih kuat daripada konsumen.

Dugaan terjadinya kebocoran data pribadi konsumen PT PLN menunjukkan bahwa PT PLN belum menjalankan prinsip-prinsip perlindungan data pribadi yang efektif terhadap akses dan pengungkapan yang tidak sah. Hal ini terlihat dari fakta bahwa data pribadi konsumen PT PLN berhasil diakses oleh peretas, yang berarti data pribadi tersebut telah terpapar oleh pihak yang tidak berhak. Lebih lanjut, data pribadi yang berhasil bocor kemudian dijual oleh peretas, yang berarti peretas secara ilegal mengungkapkan Data Pribadi Konsumen PT PLN.

Dalam konteks kasus ini, korban memiliki opsi untuk melaporkan ke lembaga khusus yang akan ditetapkan oleh presiden yang bertugas menjalankan pelindungan data pribadi. Selain sanksi administratif, individu yang merasa dirugikan akibat pengungkapan data pribadi mereka dapat mengajukan tuntutan perdata. Hal ini diatur dalam Pasal 12 ayat (1) Undang-Undang Perlindungan Data Pribadi, yang memberikan hak kepada individu yang data pribadinya terkena pelanggaran untuk mengajukan gugatan dan meminta ganti rugi sesuai dengan ketentuan undang-undang. Pengguna yang merasa dirugikan juga dapat menggugat berdasarkan Pasal 1365 Kitab Undang-Undang Hukum Perdata (KUHPerdata) tentang perbuatan melawan hukum.

Dalam situasi tersebut, pengguna (korban) memiliki dasar hukum untuk melaporkan dengan dasar wanprestasi, yang merujuk pada kelalaian perusahaan dalam memenuhi perjanjian awal antara konsumen dan perusahaan. Dalam konteks ini, korban dapat menggugat berdasarkan prinsip wanprestasi, dengan sanksi hukum yang mencakup:

- Kewajiban membayar ganti rugi kepada pihak yang dirugikan, sebagaimana diatur dalam Pasal 1243 KUHPerdata.
- Kemungkinan pembatalan perjanjian berdasarkan Pasal 1266 atau Pasal 138 ayat (2) KUHPerdata.
- Peralihan risiko akibat Force Majeure yang dapat menyebabkan wanprestasi.
- Kewajiban membayar biaya perkara yang hanya dapat diminta setelah terbukti di muka hakim dengan penetapan dari hakim.

Selain itu, berdasarkan Pasal 64 ayat (1), (2), (3), (4) Undang-Undang Perlindungan Data Pribadi, penyelesaian sengketa Perlindungan Data Pribadi dapat dilakukan melalui arbitrase, pengadilan, atau lembaga penyelesaian sengketa alternatif lainnya sesuai dengan peraturan perundang-undangan yang berlaku. Proses peradilan Perlindungan Data Pribadi sesuai dengan hukum acara yang berlaku, sejalan dengan ketentuan perundang-undangan yang berlaku, dan persidangan dilakukan secara tertutup demi menjaga kerahasiaan data pribadi.

Latihan Soal 1

1. Sebutkan fokus Kerangka hukum yang mengatur keamanan digital!
2. Sebutkan Peraturan pemerintah Indonesia mengatur keamanan data pribadi!
3. Bagiamana cara menganalisa pebedaan Kejahatan data pribadi dengan Kejahatan Keamanan Siber?

Apabila belum berhasil menjawab silahkan pelajari kembali materi terkait kerangka hukum keamanan digital pada Buku sebelumnya. Selamat berlatih.

Rangkuman

Dari uraian diatas dapat diambil kesimpulan bahwa:

Kerangka hukum yang mengatur keamanan digital mencakup beberapa aspek kunci, termasuk hak privasi, hak cipta dan kekayaan intelektual, hukum kontrak elektronik, serta hukum komunikasi elektronik. Ini bertujuan untuk melindungi hak individu dan organisasi dalam dunia digital yang semakin kompleks, dengan aturan yang mengatur keamanan data, hak privasi, dan penggunaan teknologi digital yang sah. Di Indonesia, peraturan-peraturan ini termasuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Pelaksanaan UU ITE, serta Perlindungan Data Pribadi. Perlindungan data pribadi diatur dalam UU ITE dan peraturan yang lebih rinci dalam Peraturan Pemerintah Nomor 71 Tahun 2019. Dalam dunia yang terus berkembang ini, pemahaman tentang konsep dasar keamanan digital seperti kerentanan, ancaman, risiko, serta prinsip-prinsip pertahanan dalam kedalaman, prinsip kebutuhan terhadap prinsip paling sedikit, dan prinsip privasi by design sangat penting dalam menjaga keamanan data dan sistem dari ancaman keamanan siber.

Implikasi hukum dari pelanggaran data pribadi dan pelanggaran keamanan siber memiliki dampak signifikan. Pelanggaran data pribadi mengakibatkan pelanggaran undang-undang privasi yang dapat berujung pada denda besar oleh otoritas pengawas sesuai yurisdiksi hukum yang berlaku, serta

potensi tuntutan ganti rugi perdata oleh individu yang terkena dampak. Di sisi lain, pelanggaran keamanan siber mengakibatkan tindakan kriminal yang dapat menghasilkan sanksi pidana, seperti hukuman penjara dan denda, sesuai dengan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia. Pelaku pelanggaran keamanan siber juga dapat menghadapi tuntutan perdata dari pihak yang menderita kerugian, dan kerugian reputasi yang signifikan. Oleh karena itu, pematuhan undang-undang privasi dan keamanan siber sangat penting untuk menghindari konsekuensi hukum yang merugikan.

Terhadap kasus dugaan kebocoran data pribadi konsumen PT PLN, PT PLN bertanggung jawab atas kebocoran tersebut sebagai Pengendali Data Pribadi, baik dilakukan secara sengaja atau tidak sengaja. PT PLN tetap menjadi penanggung jawab atas dugaan kebocoran data pribadi tersebut karena melanggar Pasal 38 Undang-Undang Perlindungan Data Pribadi yang mengamanatkan Pengendali Data Pribadi untuk melindungi Data Pribadi dari pemrosesan yang tidak sah. Tanggung jawab tersebut didasarkan pada Pasal 1365 Kitab Undang-Undang Hukum Perdata yang bertujuan untuk mengembalikan individu yang menderita kerugian akibat perbuatan melawan hukum kepada keadaan semula. KUH Perdata memberikan hak kepada pemohon untuk meminta ganti rugi atas kerugian materiil yang nyata maupun kerugian immateriil yang mungkin akan dideritanya di kemudian hari.

Tes Formatif 1

Pilihlah salah satu jawaban yang benar dari soal evaluasi materi berikut dengan dilingkari atau disilang.

1. Apa yang mencakup hak privasi dalam konteks hukum digital?

a. Hak atas informasi publik
b. Hak individu terhadap privasi dalam dunia digital
c. Hak untuk mengakses internet gratis
d. Hak atas kekayaan intelektual

2. Apa yang diatur oleh hukum hak cipta dalam konteks digital?

a. Hak individu terhadap privasi
b. Hak atas kekayaan intelektual dalam konten digital
c. Hak untuk berbicara secara bebas di internet
d. Hak untuk berbelanja online

3. Apa yang diatur oleh hukum kontrak elektronik?

a. Validitas dan penegakan kontrak yang dibuat secara elektronik
b. Penggunaan media sosial dalam bisnis
c. Hak individu terhadap privasi digital
d. Perlindungan data pribadi dalam dunia digital

4. Apa yang diatur oleh hukum komunikasi elektronik?

a. Hak individu terhadap privasi dalam dunia digital
b. Perlindungan hak cipta dalam komunikasi elektronik
c. Validitas kontrak dalam email
d. Regulasi untuk perdagangan internasional

5. Apa yang dimaksud dengan konsep dasar keamanan digital "kerahasiaan"?

a. Menjaga informasi agar tidak bocor kepada pihak yang tidak berkepentingan
b. Memastikan totalitas perusahaan dalam transaksi
c. Membuat keputusan yang menghormati diri sendiri dan orang lain secara online
d. Hak individu terhadap privasi dalam dunia digital

6. Apa yang mencakup implikasi hukum dari pelanggaran data pribadi?

a. Hanya denda finansial
b. Sanksi pidana bagi pelaku
c. Hanya mengakibatkan kerugian finansial bagi individu
d. Sanksi finansial dan perdata, tergantung pada tingkat pelanggaran dan yurisdiksi hukum yang berlaku.

7. Apa yang dimaksud dengan undang-undang kejahatan siber dan mengapa itu penting?

a. Undang-undang yang mengatur pembuatan perangkat lunak keamanan
b. Undang-undang yang melarang penggunaan internet
c. Undang-undang yang mengatur tindakan kriminal dalam keamanan siber dan penting untuk penyelidikan dan penuntutan pelaku.
d. Undang-undang yang hanya berlaku di Amerika Serikat

8. Undang-undang mana yang mengatur hak privasi dan perlindungan data pribadi di Uni Eropa?

a. Undang-undang Privasi Konsumen California (CCPA)
b. Undang-undang Informasi dan Transaksi Elektronik (UU ITE) di Indonesia
c. Regulasi Perlindungan Data Umum (GDPR)
d. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

9. Apa yang mungkin menjadi konsekuensi hukum bagi pelaku pelanggaran keamanan siber di Indonesia menurut Undang-Undang Informasi dan Transaksi Elektronik (UU ITE)?

a. Sanksi perdata
b. Denda yang rendah
c. Hukuman penjara
d. Kehilangan pekerjaan

10. Mengapa penting untuk memahami konsep dasar dalam keamanan digital, seperti "kerahasiaan" dan "integritas"?

a. Hanya untuk tujuan akademik
b. Untuk menghindari pajak
c. Untuk memahami bagaimana melindungi sistem dan data dalam

lingkungan **digital**

d. Untuk mengurangi risiko dalam berbelanja online

Umpan Balik

Cocokan jawaban anda dengan Kunci Jawaban. Hitunglah jawaban anda yang benar, kemudian gunakan rumus di bawah ini untuk mengetahui tingkat penguasaan anda terhadapmateri Buku.

Untuk latihan soal, setiap soal memiliki bobot nilai yang sama, yaitu 10/soal.

Tes formatif:

Arti tingkat penguasaan yang Anda capai:

90 – 100 % = baik sekali

80 – 89 % = baik

70 – 79 % = cukup

< 70 % = kurang

Tindak lanjut

Bila anda mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan ke materi selanjutnya. Tetapi bila tingkat penguasaan anda masih di bawah 80%, Anda harus mengulangi materi Buku, terutama bagian yang belum anda kuasai.

MATERI

II

ANCAMAN KEAMANAN SIBER

Indikator Keberhasilan

Setelah mempelajari Materi 2 tentang Ancaman Kemanan Siber ini indikator keberhasilan adalah apabila anda dapat:

- Mengidentifikasi Malware dan Serangan Perangkat Lunak Berbahaya
- Mengidentifikasi Serangan DDoS (Distributed Denial of Service)
- Mampus memahami dan menjelasakan Phishing dan Serangan Sosial

A. Malware dan Serangan Perangkat Lunak Berbahaya

1. Pengertian Malware

Malware adalah singkatan dari malicious software, yaitu program komputer yang dirancang untuk merusak, mengganggu, atau mencuri data dari sistem komputer tanpa izin pengguna. Malware dapat berupa virus, worm, trojan, spyware, adware, dan ransomware. Virus adalah program yang menyebar dengan menempel pada file lain dan dapat merusak sistem komputer. Worm adalah program yang menyebar melalui jaringan dan dapat menginfeksi banyak komputer dalam waktu singkat. Trojan adalah program yang menyamar sebagai program yang berguna tetapi sebenarnya memiliki tujuan jahat. Spyware adalah program yang dirancang untuk mencuri informasi pribadi pengguna. Adware adalah program yang menampilkan iklan yang tidak diinginkan pada sistem komputer. Ransomware adalah program

yang mengenkripsi data pada sistem komputer dan meminta tebusan untuk mendapatkan kunci dekripsi. Malware dapat merusak sistem komputer, mencuri data pribadi, dan mengganggu kinerja sistem komputer. Oleh karena itu, pengguna perlu menginstal perangkat lunak keamanan dan menghindari mengunduh atau membuka lampiran email yang mencurigakan untuk mencegah infeksi malware pada sistem komputer.

2. Jenis-Jenis Malware

Malware atau malicious software adalah program berbahaya yang berjalan di dalam sebuah sistem komputer tanpa izin dengan tujuan untuk merusak atau mencuri data pribadi dari sistem. Perkembangan malware yang semakin pesat, menyebabkan banyak jenis keluarga malware baru yang bermunculan. Beberapa jenis malware yang ada antara lain virus, worm, trojan, spyware, adware, ransomware, backdoor, rootkit, botnet, fileless malware, banking trojan, dan cryptojacking malware. Setiap jenis malware memiliki karakteristik dan tujuan yang berbeda-beda. Untuk mencegah infeksi malware pada sistem komputer, pengguna perlu menginstal perangkat lunak keamanan dan menghindari mengunduh atau membuka lampiran email yang mencurigakan. Selain itu, pengguna juga perlu mengetahui jenis-jenis malware yang ada agar dapat mengenali tanda-tanda infeksi malware pada sistem komputer.

3. Cara Penyebaran Malware

Penyebaran malware dapat terjadi melalui berbagai cara, seperti melalui email, situs web yang tidak aman, perangkat lunak yang tidak resmi, dan media penyimpanan yang terinfeksi. Berikut adalah beberapa cara penyebaran malware yang lebih spesifik:

- Melalui jaringan komputer: malware dapat menyebar melalui jaringan komputer dengan memanfaatkan celah keamanan pada sistem atau perangkat lunak yang digunakan.
- Melalui media penyimpanan: malware dapat menyebar melalui media penyimpanan seperti flashdisk, CD, atau DVD yang terinfeksi.
- Melalui email: malware dapat menyebar melalui lampiran email yang mencurigakan atau melalui tautan yang mengarah ke situs web yang tidak aman.
- Melalui situs web yang tidak aman: malware dapat menyebar melalui situs web yang tidak aman atau melalui iklan yang terinfeksi pada situs web tersebut.
- Melalui perangkat lunak yang tidak resmi: malware dapat disisipkan pada perangkat lunak yang tidak resmi atau bajakan yang diunduh dari internet.
- Melalui social engineering: malware dapat menyebar melalui teknik social engineering yang memanfaatkan kelemahan manusia untuk meminta pengguna untuk menginstal perangkat lunak yang sebenarnya berisi malware. Untuk mencegah penyebaran malware, pengguna perlu menghindari mengunduh atau membuka lampiran email yang mencurigakan, menginstal perangkat lunak keamanan, dan menghindari mengunjungi situs web yang tidak aman.

4. Dampak Malware

Malware dapat memberikan dampak yang merugikan bagi pengguna sistem komputer. Berikut adalah beberapa dampak yang dapat ditimbulkan oleh malware:

- Merusak sistem komputer: malware dapat merusak sistem komputer dengan menghapus atau merusak file sistem yang penting.
- Mencuri data pribadi: malware dapat mencuri data pribadi seperti informasi login, nomor kartu kredit, dan informasi pribadi lainnya.
- Mengganggu kinerja sistem komputer: malware dapat mengganggu kinerja sistem komputer dengan memakan sumber daya komputer yang berlebihan.
- Menyebar ke sistem komputer lain: beberapa jenis malware seperti worm dan botnet dapat menyebar ke sistem komputer lain melalui jaringan komputer.
- Membuat sistem komputer rentan terhadap serangan lain: malware dapat membuka celah keamanan pada sistem komputer sehingga membuat sistem komputer rentan terhadap serangan lain.
- Membuat pengguna sistem komputer menjadi korban kejahatan: beberapa jenis malware seperti ransomware dapat membuat pengguna sistem komputer menjadi korban kejahatan dengan meminta tebusan untuk mendapatkan kunci dekripsi data yang telah dienkripsi. Oleh karena itu, pengguna perlu menginstal perangkat lunak keamanan dan menghindari mengunduh atau membuka lampiran email yang mencurigakan untuk mencegah infeksi malware pada sistem komputer. Selain itu, pengguna juga perlu melakukan backup data secara teratur untuk menghindari kehilangan data akibat infeksi malware.

5. Upaya Penanggulangan dan Pencegahan

Dalam perspektif hukum Indonesia, upaya penanggulangan dan pencegahan malware melibatkan sejumlah regulasi dan peraturan yang bertujuan untuk melindungi masyarakat dari serangan perangkat lunak berbahaya. Hukum Cybercrime, yang mencakup UU ITE (Undang-Undang Informasi dan Transaksi Elektronik), menegaskan tindakan ilegal terkait dengan kejahatan siber, termasuk penyebaran malware. Penegakan hukum di Indonesia dapat melibatkan tindakan hukum terhadap pelaku yang terlibat dalam pembuatan, penyebaran, atau penggunaan malware dengan niat jahat. Selain itu, pemerintah dan lembaga terkait telah mengembangkan pedoman keamanan siber dan bekerjasama dengan sektor swasta untuk meningkatkan kesadaran dan keterlibatan dalam praktik keamanan siber yang efektif, seiring dengan upaya untuk menciptakan kerangka hukum yang lebih komprehensif untuk mengatasi ancaman keamanan siber.

Lembar Kerja

Tabel 3. Matrik Diskusi Malware dan Serangan Perangkat Lunak Berbahaya

Poin diskusi	Deskripsi
Jenis Malware	Diskusikanlah apa saja jenis-jenis malware yang perlu diperhatikan, bagaimana cara kerja masing-masing jenis malware serta apa tujuan dari setiap jenis malware tersebut.
Metode Penyebaran	Diskusikanlah bagaimana malware menyebar dari satu perangkat ke perangkat lainnya, Apa saja metode penyebaran malware yang umum

	digunakan saat ini serta apakah ada tren baru dalam metode penyebaran malware yang perlu diwaspadai.
Dampak	Diskusikanlah apa dampak dari serangan malware terhadap perangkat lunak dan system, bagaimana malware mempengaruhi pengguna dan organisasi secara keseluruhan, serta apa saja kerugian finansial dan non-finansial yang mungkin terjadi akibat serangan malware.
Deteksi dan Pencegahan	Diskusikanlah Apa metode deteksi yang efektif untuk mengidentifikasi keberadaan malware, bagaimana organisasi dapat mencegah serangan malware secara proaktif, serta apa peran teknologi kecerdasan buatan (AI) dalam deteksi dan pencegahan malware.
Tanggung Jawab	Diskusikanlah siapa yang bertanggung jawab atas keamanan terhadap serangan malware di suatu organisasi, bagaimana peran individu, organisasi, dan pemerintah dalam memitigasi risiko malware, serta apakah terdapat standar atau regulasi yang harus dipatuhi untuk melindungi perangkat lunak dari serangan malware.
Evolusi Malware	Diskusikanlah bagaimana evolusi malware dari waktu ke waktu, apa yang dapat dipelajari dari serangan malware masa lalu untuk meningkatkan

	keamanan di masa mendatang, serta apakah tren terkini dalam pengembangan malware menunjukkan perubahan atau peningkatan dalam teknik atau tujuan serangan.

B. Serangan DDoS (Distributed Denial of Service)

1. Pengertian Serangan DDoS (Distributed Denial of Service)

Serangan DDoS (Distributed Denial of Service) adalah serangan terhadap suatu sistem komputer atau jaringan yang bertujuan untuk membuat layanan atau sumber daya tidak tersedia bagi pengguna yang sah. Serangan ini mencoba mengganggu ketersediaan layanan dengan membanjiri sistem atau jaringan target dengan lalu lintas data yang berlebihan, sehingga menyebabkan layanan tidak dapat diakses oleh pengguna yang sebenarnya.

Cara kerja dari serangan DDoS melibatkan penggunaan banyak perangkat atau komputer yang terhubung dalam suatu jaringan untuk secara bersama-sama mengirimkan sejumlah besar permintaan atau lalu lintas ke target secara bersamaan. Tujuannya adalah untuk menghabiskan sumber daya sistem target seperti bandwidth jaringan, kapasitas pemrosesan, atau sumber daya lainnya sehingga layanan tidak dapat diakses oleh pengguna yang sah.

Tabel 4. Langkah-langkah umum dalam serangan DDoS

Rekrutmen Botnet	Para pelaku serangan biasanya mengendalikan jaringan perangkat yang sudah terinfeksi malware atau telah dikompromi sebelumnya. Jaringan perangkat ini dikenal sebagai botnet. Botnet dapat terdiri

	dari ribuan hingga jutaan perangkat, termasuk komputer, server, atau perangkat IoT yang telah diretas.
Pengiriman Lalu Lintas Berlebihan	Setelah memiliki botnet yang cukup besar, para penyerang mengirimkan lalu lintas data yang besar ke target secara bersamaan. Hal ini dapat dilakukan dengan menggunakan berbagai metode, seperti serangan dengan protokol HTTP, UDP, SYN, dan lainnya, yang mengakibatkan kelebihan beban pada sumber daya komputasi atau jaringan target.
Penyumbatan Jaringan atau Sumber Daya	Akibat dari banjir lalu lintas yang tidak wajar ini, sistem atau jaringan target menjadi tidak responsif terhadap permintaan layanan yang sebenarnya. Hal ini bisa membuat layanan menjadi lambat atau bahkan tidak dapat diakses sama sekali bagi pengguna yang sah.
Kesulitan Identifikasi Sumber Serangan	Serangan DDoS sering kali sulit untuk diidentifikasi karena datang dari berbagai sumber yang terdistribusi di seluruh dunia. Penyerang bisa menggunakan teknik tertentu untuk menyembunyikan asal serangan, membuatnya lebih sulit untuk dihalau.

Seringkali, serangan DDoS digunakan untuk meminta uang tebusan (ransom) kepada pemilik sistem yang diserang, atau sebagai alat untuk mengganggu layanan pada suatu organisasi atau entitas tertentu.

Serangan DDoS dianggap sebagai ancaman yang signifikan karena kemampuannya untuk secara massal membanjiri target dengan lalu lintas data yang berlebihan, menyebabkan layanan menjadi tidak tersedia bagi pengguna yang sah. Dampaknya tidak hanya terbatas pada gangguan operasional, tetapi juga mencakup kerugian finansial yang besar, kerusakan reputasi perusahaan, dan bahkan potensi gangguan terhadap infrastruktur kritis seperti layanan perbankan, pemerintahan, atau kesehatan. Selain itu, serangan ini sulit diidentifikasi asalnya dan membutuhkan solusi keamanan canggih untuk memitigasinya,

menjadikannya sebagai ancaman yang serius terhadap stabilitas dan keamanan sistem digital di era saat ini.

2. Jenis Serangan

Terdapat beberapa jenis serangan DDoS yang umum digunakan oleh para penyerang untuk mengganggu layanan online. Pertama, serangan Flood merupakan jenis yang paling umum, di mana penyerang membanjiri target dengan lalu lintas data palsu atau permintaan koneksi yang tak terbatas. Jenis ini termasuk serangan UDP flood, SYN flood, dan HTTP flood. Selanjutnya, serangan Amplifikasi memanfaatkan layanan yang dapat memberikan tanggapan besar terhadap permintaan kecil, seperti serangan DNS amplifikasi atau NTP amplifikasi. Ada pula serangan Volumetric, yang bertujuan menghabiskan bandwidth jaringan dengan lalu lintas data yang sangat tinggi. Serta, serangan Aplikasi, yang menyerang kelemahan pada aplikasi atau layanan tertentu untuk membebani sumber daya perangkat lunak, seperti serangan HTTP POST atau Slowloris.

Dalam mengklasifikasikan serangan DDoS berdasarkan metode serangannya, ada tiga kategori utama. Pertama, Metode Lapisan Jaringan (Network Layer) yang menargetkan infrastruktur jaringan dengan serangan SYN flood, UDP flood, atau ICMP flood. Kedua, Metode Lapisan Transport (Transport Layer) yang memanfaatkan protokol transport, seperti serangan TCP flood. Terakhir, Metode Lapisan Aplikasi (Application Layer) yang menyasar layanan atau aplikasi yang berjalan di atas protokol, seperti serangan HTTP flood atau Slowloris.

Variasi dalam skala dan kompleksitas serangan DDoS juga perlu dipertimbangkan. Skala serangan bisa bervariasi mulai dari serangan kecil yang menargetkan satu sasaran hingga serangan besar yang menyerang infrastruktur besar seperti penyedia layanan cloud atau perusahaan besar. Sementara itu, kompleksitas serangan terus berkembang seiring peningkatan teknologi. Para penyerang mengembangkan metode baru dan serangan yang lebih kompleks, menggunakan botnets yang lebih kuat, teknik penyembunyian sumber, atau bahkan memanfaatkan kecerdasan buatan untuk mengelabui sistem pertahanan. Oleh karena itu, pembaruan strategi keamanan secara berkala menjadi penting untuk menghadapi ancaman DDoS yang semakin canggih.

3. Tujuan Serangan

Pelaku serangan DDoS memiliki beberapa tujuan yang mendasari tindakan mereka. Pertama, tujuan utamanya adalah untuk membuat layanan atau sumber daya yang menjadi target tidak tersedia bagi pengguna yang sah. Ini bisa dimotivasi oleh hasrat untuk menciptakan ketidakstabilan, menyebabkan ketidaknyamanan, atau merusak reputasi target. Serangan DDoS juga dapat digunakan sebagai alat untuk memeras uang tebusan (ransom) dari korban dengan ancaman akan melanjutkan serangan jika pembayaran tidak dilakukan.

Serangan DDoS dapat menyebabkan kerugian yang signifikan bagi organisasi atau individu yang menjadi target. Kerugian tersebut mencakup penurunan ketersediaan layanan, yang dapat mengganggu operasional bisnis dan menimbulkan dampak finansial. Selain itu, serangan semacam itu juga dapat merusak reputasi organisasi karena pelanggan atau

pengguna mungkin kehilangan kepercayaan terhadap layanan yang tidak stabil atau sering tidak tersedia. Selain itu, dalam beberapa kasus, serangan DDoS terhadap infrastruktur kritis seperti layanan kesehatan atau perbankan dapat menyebabkan gangguan yang berdampak pada keamanan dan kesejahteraan masyarakat secara keseluruhan.

Motivasi di balik serangan DDoS dapat sangat bervariasi. Beberapa serangan memiliki motif ekonomi, di mana penyerang ingin mendapatkan keuntungan finansial baik melalui pemerasan atau persaingan bisnis yang tidak sehat. Motivasi politik juga dapat menjadi faktor, di mana serangan dilakukan untuk mengekspresikan ketidakpuasan terhadap suatu kebijakan atau organisasi tertentu. Selain itu, terdapat serangan yang dilakukan atas dasar ideologi, di mana pelaku berupaya mempengaruhi opini publik atau menciptakan gangguan atas dasar keyakinan atau ide tertentu.

4. Sumber Serangan

Sumber serangan DDoS umumnya berasal dari berbagai lokasi dan perangkat yang tersebar di seluruh dunia. Penyerang memanfaatkan perangkat yang terinfeksi malware, seperti komputer, server, perangkat IoT, atau bahkan perangkat yang disusupi oleh botnets. Perangkat-perangkat ini dapat dikuasai dari jarak jauh oleh penyerang, yang kemudian menggunakan mereka sebagai alat untuk melancarkan serangan DDoS. Bagian terbesar dari serangan DDoS ini sering kali berasal dari botnets, yaitu jaringan perangkat yang terhubung dan dikendalikan oleh penyerang. Botnets dapat mencakup ribuan hingga jutaan perangkat yang rentan dan terinfeksi, dan dengan koordinasi yang

terpusat atau terdistribusi, mereka memungkinkan penyerang untuk mengirimkan lalu lintas data yang berlebihan ke target secara simultan, membanjiri infrastruktur atau layanan yang menjadi sasaran serangan. Kekuatan dan skala dari serangan DDoS ini sering kali tergantung pada ukuran dan kekuatan botnets yang digunakan oleh penyerang, memperumit upaya identifikasi serta penanganan sumber serangan.

5. Deteksi dan Mitigasi

Untuk mendeteksi serangan DDoS sedini mungkin, perlu digunakan sistem pemantauan yang canggih untuk memonitor lalu lintas jaringan secara terus-menerus. Dengan menganalisis pola lalu lintas yang tidak biasa, seperti lonjakan tak terduga dalam jumlah permintaan atau jenis permintaan yang tidak lazim, sistem pemantauan dapat memberikan peringatan dini terhadap potensi serangan DDoS. Selain itu, penggunaan perangkat lunak atau perangkat keras yang dirancang khusus untuk mendeteksi perilaku serangan DDoS seperti alat mitigasi, firewall, atau Intrusion Prevention System (IPS) dapat membantu dalam mendeteksi serangan tersebut dengan cepat.

Ketika serangan DDoS terjadi, langkah-langkah yang dapat diambil untuk mengurangi dampaknya termasuk melakukan proteksi pada infrastruktur jaringan dan server dengan konfigurasi yang lebih kuat, mempertimbangkan untuk memblokir lalu lintas yang berasal dari sumber yang mencurigakan, atau mengalihkan lalu lintas yang terkena serangan ke layanan penyaringan untuk membersihkan lalu lintas jaringan dari serangan tersebut. Pembaruan atau konfigurasi ulang sementara pada sistem, pemantauan intensif terhadap lalu lintas jaringan, dan komunikasi

yang efektif dengan penyedia layanan hosting atau ISP juga merupakan langkah penting dalam mengurangi dampak serangan DDoS.

Terdapat beberapa teknologi dan layanan khusus yang efektif dalam melindungi infrastruktur dari serangan DDoS. Salah satunya adalah layanan mitigasi DDoS yang disediakan oleh penyedia layanan keamanan atau CDN (Content Delivery Network). Layanan ini mampu mendeteksi dan memblokir lalu lintas yang mencurigakan atau yang terlibat dalam serangan DDoS sebelum mencapai infrastruktur yang sebenarnya. Selain itu, teknologi seperti scrubbing centers atau scrubbing services, yang merupakan fasilitas khusus yang membersihkan lalu lintas jaringan dari serangan DDoS sebelum mengalir ke infrastruktur internal, juga membantu dalam melindungi dan memitigasi dampak serangan tersebut.

6. Kerugian

Serangan DDoS dapat memiliki dampak yang merusak terhadap layanan atau infrastruktur yang menjadi target. Dampak utamanya adalah penurunan ketersediaan layanan, yang mengakibatkan layanan menjadi tidak dapat diakses bagi pengguna yang sah. Infrastruktur yang diserang dapat mengalami gangguan yang menyebabkan situs web, aplikasi, atau layanan online menjadi tidak responsif atau lambat, bahkan sampai tidak bisa diakses sama sekali. Selain itu, serangan DDoS dapat merusak server atau perangkat keras, menyebabkan kerusakan pada jaringan, dan mengganggu aktivitas operasional secara keseluruhan.

Pengaruh serangan DDoS terhadap reputasi dan kinerja suatu organisasi dapat signifikan. Dalam pandangan publik, serangan yang sering terjadi atau layanan yang tidak stabil dapat merusak citra

perusahaan atau organisasi tersebut. Pelanggan atau pengguna yang kesulitan mengakses layanan dapat kehilangan kepercayaan terhadap keseriusan perusahaan dalam menjaga kehandalan layanan. Hal ini bisa berdampak pada kehilangan pelanggan, penurunan loyalitas, atau bahkan berpotensi menyebabkan gangguan pada kerja sama bisnis atau kemitraan strategis.

Secara finansial, serangan DDoS dapat menimbulkan kerugian yang signifikan bagi organisasi atau perusahaan. Biaya yang timbul dari pemulihan infrastruktur yang rusak, investasi dalam solusi keamanan tambahan untuk menghindari serangan masa depan, atau bahkan kehilangan pendapatan akibat layanan yang tidak tersedia selama serangan dapat sangat merugikan. Perusahaan juga bisa mengalami kerugian finansial karena berkurangnya transaksi atau penjualan, serta biaya tambahan yang dikeluarkan untuk mengatasi dan memulihkan layanan yang terganggu.

7. Pencegahan

Untuk mengurangi risiko serangan DDoS, langkah-langkah pencegahan yang dapat diambil meliputi penerapan teknologi perlindungan seperti firewall yang kuat, perangkat lunak anti-DDoS, atau layanan mitigasi yang disediakan oleh penyedia layanan keamanan. Selain itu, diversifikasi infrastruktur dengan menggunakan layanan CDN (Content Delivery Network) atau DNS (Domain Name System) yang dapat menyebar beban lalu lintas dan memiliki kemampuan mitigasi dapat membantu melindungi dari serangan DDoS. Pemantauan lalu lintas jaringan secara teratur juga penting, sehingga dapat mendeteksi dan

menanggapi serangan secepat mungkin, sementara melakukan perbaikan atau penyesuaian konfigurasi infrastruktur sesuai dengan tren serangan yang terjadi.

Pentingnya perencanaan dan kebijakan keamanan dalam melindungi dari serangan DDoS sangat besar. Perencanaan keamanan yang komprehensif memungkinkan organisasi untuk mengidentifikasi risiko, menetapkan prioritas perlindungan, dan menetapkan langkah-langkah yang harus diambil dalam menanggapi serangan DDoS. Kebijakan keamanan yang jelas dan terstruktur akan memandu organisasi dalam menjalankan praktik terbaik untuk melindungi infrastruktur mereka, menetapkan prosedur tanggap darurat, serta memperjelas peran dan tanggung jawab tim keamanan dalam menghadapi dan menanggapi serangan DDoS dengan efisien.

Pelatihan dan pendidikan bagi staf IT atau keamanan merupakan aspek penting dalam menghadapi serangan DDoS. Staf harus diberikan pemahaman yang mendalam tentang jenis serangan yang mungkin terjadi, cara mendeteksi serangan DDoS secara dini, serta langkah-langkah mitigasi yang dapat diambil. Pelatihan ini dapat mencakup simulasi serangan, peningkatan keterampilan dalam pemantauan lalu lintas jaringan, dan pemahaman tentang alat dan teknologi yang digunakan untuk melindungi dan mengatasi serangan DDoS. Meningkatkan pengetahuan dan keterampilan staf akan membantu dalam respons yang cepat dan efektif saat menghadapi serangan tersebut.

C. Phishing dan Serangan Sosial

1. Pengertian Phising dan Serangan Sosial

Phishing adalah jenis serangan cyber yang melibatkan upaya penipuan untuk memperoleh informasi sensitif atau data pribadi dari individu atau organisasi dengan menyamar sebagai entitas tepercaya. Teknik yang umum digunakan dalam phishing termasuk pengiriman email, pesan teks, atau komunikasi online lainnya yang menyerupai komunikasi resmi dari lembaga keuangan, perusahaan, atau organisasi yang dikenal. Para penyerang sering berpura-pura menjadi entitas yang sah untuk merayu korbannya agar memberikan informasi rahasia seperti kata sandi, informasi kartu kredit, nomor identitas, atau data keuangan lainnya. Tujuan utama dari serangan phishing adalah untuk mencuri informasi pribadi atau keuangan, mengakses akun pengguna, melakukan penipuan keuangan, atau bahkan menjalankan serangan yang lebih luas seperti pencurian identitas atau serangan terhadap infrastruktur organisasi.

Serangan sosial adalah bentuk serangan cyber yang menggunakan manipulasi psikologis atau interaksi sosial untuk memanipulasi individu atau kelompok dengan tujuan memperoleh informasi sensitif, akses ke sistem, atau merusak reputasi. Teknik yang digunakan dalam serangan sosial sering melibatkan upaya penipuan, manipulasi, atau pemalsuan identitas untuk mendapatkan kepercayaan individu. Ini dapat terjadi melalui berbagai saluran komunikasi, termasuk telepon, email, pesan teks, atau media sosial. Tujuan utama dari serangan ini bisa bermacam-macam, mulai dari mendapatkan akses ke sistem atau informasi rahasia, mencuri data sensitif, memanipulasi individu agar melakukan tindakan

tertentu, hingga merusak reputasi individu atau organisasi dengan menyebarkan informasi palsu atau memanfaatkan informasi yang sensitif. Serangan sosial sering kali menyasar aspek psikologis dan sosial, menggunakan teknik manipulasi dan persuasi untuk mencapai tujuan penyerangnya.

2. Perbedaan Phising dan Serangan Sosial

a. Pendekatan

- Phishing: Pendekatan dalam phishing lebih cenderung terfokus pada penggunaan pesan palsu atau komunikasi yang menipu untuk menipu individu atau organisasi agar memberikan informasi pribadi atau keuangan.
- Serangan Sosial: Serangan sosial menggunakan pendekatan yang lebih luas, termasuk penggunaan manipulasi psikologis atau interaksi sosial langsung untuk memanipulasi individu atau kelompok agar melakukan tindakan tertentu atau membagikan informasi rahasia.

b. Metode

- Phishing: Metode utama dalam phishing adalah melalui pesan teks, email, atau komunikasi online yang meniru entitas yang dikenal dengan tujuan untuk mendapatkan informasi sensitif.
- Serangan Sosial: Serangan sosial dapat menggunakan metode yang lebih beragam, termasuk komunikasi telepon, obrolan langsung, atau interaksi langsung dengan individu atau kelompok untuk memanipulasi mereka.

c. Sasaran

- Phishing: Sasaran utama dari phishing adalah mendapatkan informasi sensitif seperti kata sandi, informasi keuangan, atau data pribadi dengan merayu korban untuk memberikannya.
- Serangan Sosial: Sasaran serangan sosial bisa lebih beragam, mulai dari mendapatkan akses ke sistem atau informasi rahasia, mempengaruhi tindakan tertentu, hingga merusak reputasi individu atau organisasi.

Dalam konteks ini, meskipun keduanya memiliki kesamaan dalam upaya memperoleh informasi sensitif, phishing lebih terfokus pada teknik penipuan dalam komunikasi digital, sementara serangan sosial menggunakan metode yang lebih luas, termasuk manipulasi psikologis dan interaksi sosial langsung untuk mencapai tujuan yang beragam.

3. Ciri-Ciri Umum Dari Email Atau Pesan Phishing

Terdapat beberapa ciri-ciri umum dalam email phishing yang perlu diperhatikan untuk mengidentifikasi pesan yang mencurigakan:

a Tautan yang mencurigakan atau URL yang tidak sah: Email phishing sering kali mengandung tautan atau URL yang terlihat asing, tidak relevan dengan isi pesan, atau menuntun ke situs web palsu yang mencoba meniru situs resmi. Periksa alamat URL dengan hati-hati sebelum mengkliknya, dan pastikan untuk memverifikasi keasliannya jika ada keraguan.

b Tekanan waktu atau urgensi: Pesan phishing sering menciptakan tekanan waktu atau urgensi bagi penerima dengan menyatakan bahwa tindakan harus segera dilakukan, misalnya, "Tindakan segera

diperlukan" atau "Jika Anda tidak segera merespons, akun Anda akan dinonaktifkan." Hal ini dimaksudkan untuk memaksa penerima agar bertindak tanpa mempertimbangkan dengan seksama.

c Permintaan informasi pribadi atau sensitif: Email phishing seringkali meminta informasi pribadi atau sensitif seperti kata sandi, nomor kartu kredit, informasi akun bank, atau data pribadi lainnya. Perusahaan atau organisasi yang sah jarang akan meminta informasi sensitif melalui email, terutama jika itu datang secara tak terduga atau tanpa alasan yang jelas.

d Bahasa yang mengintimidasi atau tidak profesional: Pesan phishing seringkali menggunakan bahasa yang terlalu mengintimidasi, tidak profesional, atau memiliki kesalahan tata bahasa yang mencolok. Email yang sah biasanya menggunakan bahasa yang lebih resmi dan terstruktur dengan baik.

e Lampiran atau file yang mencurigakan: Email phishing juga dapat mengandung lampiran atau file yang mencurigakan. Hindari membuka lampiran dari email yang tidak Anda kenal atau tidak Anda harapkan, karena bisa mengandung malware atau virus yang membahayakan.

4. Alasan Phishing Dianggap Sebagai Ancaman Keamanan Yang Serius

Serangan phishing memiliki dampak yang merugikan baik bagi individu maupun perusahaan. Secara individu, serangan ini dapat mengakibatkan kehilangan data pribadi seperti kata sandi, informasi keuangan, atau rahasia identitas, yang pada gilirannya bisa dimanfaatkan untuk pencurian identitas atau penipuan finansial. Dampaknya juga dapat dirasakan oleh perusahaan atau organisasi dengan merusak reputasi,

kehilangan kepercayaan pelanggan, dan potensi kerugian finansial akibat gangguan operasional atau penyalahgunaan informasi yang diakses melalui serangan tersebut. Serangan phishing begitu efektif karena mereka mengeksploitasi aspek psikologis manusia, menggiring individu atau karyawan untuk memberikan informasi sensitif dengan menyamar sebagai entitas yang terpercaya atau menciptakan situasi yang mendesak untuk bertindak cepat tanpa pertimbangan yang cermat. Keberhasilan serangan phishing seringkali bergantung pada kelalaian atau kecerobohan manusia, dan para penyerang terus mengembangkan teknik mereka untuk membuat pesan atau situs palsu mereka semakin meyakinkan. Hal ini menjadikan serangan ini sebagai salah satu ancaman yang efektif dan sulit untuk dikenali oleh banyak individu atau organisasi.

5. Dampak Serangan Sosial Pada Individu dan Organisasi

Serangan sosial memiliki dampak yang serius terhadap kepercayaan, reputasi, dan keamanan informasi, baik pada tingkat personal maupun perusahaan. Pada tingkat personal, serangan sosial dapat merusak kepercayaan individu terhadap orang atau entitas yang mereka kenal atau percayai. Penipuan sosial yang berhasil bisa mempengaruhi persepsi individu terhadap orang lain, mengakibatkan keraguan dan ketidakpercayaan dalam interaksi sosial, bahkan antara teman atau kolega dekat. Pada tingkat perusahaan, serangan sosial dapat menyebabkan kerusakan reputasi yang serius. Jika data sensitif atau informasi rahasia perusahaan bocor akibat serangan ini, hal tersebut bisa mengakibatkan hilangnya kepercayaan pelanggan, penurunan nilai merek, dan dampak finansial yang signifikan. Selain itu, keamanan informasi

perusahaan menjadi terancam karena serangan sosial seringkali memanfaatkan kesalahan manusia untuk memperoleh akses ke sistem atau informasi sensitif, memungkinkan terjadinya pencurian data atau kebocoran informasi rahasia. Kesadaran akan risiko serangan sosial serta peningkatan pemahaman dan pelatihan bagi individu dan staf perusahaan menjadi penting untuk mencegah kerugian yang lebih lanjut akibat serangan semacam ini.

Table 5. Contoh Kasus Serangan Sosial

Serangan Sosial Pada Individu	*Studi kasus serangan sosial pada individu adalah skema phishing melalui email di mana seorang karyawan menerima email yang terlihat seperti pesan dari departemen IT perusahaan. Email tersebut meminta karyawan untuk memperbarui kata sandi akun mereka melalui tautan yang disediakan. Tanpa curiga, karyawan tersebut mengklik tautan dan memasukkan informasi pribadi termasuk kata sandi. Sayangnya, email tersebut palsu dan merupakan upaya phishing yang berhasil. Penyerang berhasil mendapatkan akses ke akun karyawan dan menggunakan informasi tersebut untuk mengakses data sensitif perusahaan. Hal ini mengakibatkan pencurian informasi rahasia perusahaan, yang berdampak pada kerugian finansial dan kerusakan reputasi perusahaan karena pelanggaran keamanan data.*
Serangan Sosial Pada Organisasi	*Studi kasus serangan sosial pada organisasi, kita dapat mengamati insiden di mana seorang penyerang menyamar sebagai kontraktor atau mitra bisnis perusahaan. Dengan menggunakan informasi palsu dan memanfaatkan interaksi sosial yang ada, penyerang berhasil meyakinkan staf perusahaan untuk memberikan akses ke jaringan internal atau sistem yang sensitif. Setelah mendapatkan akses, penyerang dapat merusak data, mencuri informasi sensitif, atau bahkan menempatkan malware di dalam sistem. Serangan semacam ini dapat mengakibatkan kerugian finansial yang besar, kerusakan reputasi, dan kerugian operasional yang signifikan karena gangguan pada layanan atau infrastruktur perusahaan.*

Dari analisis dua contoh di atas menggambarkan bagaimana serangan sosial dapat merugikan baik individu maupun organisasi. Keduanya menunjukkan bagaimana manipulasi psikologis atau interaksi sosial yang dimanfaatkan oleh penyerang dapat mengakibatkan kerugian data, kebocoran informasi rahasia, kerusakan reputasi, dan potensi kerugian finansial yang serius bagi individu atau perusahaan. Kesadaran akan risiko serangan sosial dan pelatihan keamanan yang tepat sangatlah penting untuk mencegah terjadinya serangan semacam ini.

Latihan Soal 2

1. Jelaskan apa yang dimaksud dengan serangan phishing. Berikan contoh bagaimana serangan phishing dapat terjadi dan sebutkan langkah-langkah yang dapat diambil untuk menghindari serangan semacam ini.
2. erangkan konsep dari serangan ransomware. Bagaimana serangan ini bekerja dan sebutkan dampaknya terhadap individu atau organisasi. Berikan beberapa strategi yang dapat diterapkan untuk mencegah atau mengatasi serangan ransomware.
3. Jelaskan DDoS (Distributed Denial of Service) attack. Bagaimana serangan semacam ini mempengaruhi layanan online? Berikan contoh tindakan pencegahan yang bisa diambil oleh perusahaan untuk melindungi infrastruktur mereka dari serangan DDoS.
4. Terangkan mengenai peran malware dalam ancaman keamanan siber. Sebutkan beberapa jenis malware yang umum dan jelaskan cara penyebarannya serta dampak yang ditimbulkan. Berikan langkah-langkah preventif yang bisa diambil untuk melindungi sistem dari serangan malware.

Apabila belum berhasil menjawab silahkan pelajari kembali materi terkait Ancaman Keamanan Siber pada Buku. Selamat berlatih.

Rangkuman

Dari uraian diatas dapat diambil kesimpulan bahwa:

Malware, atau malicious software, merupakan program komputer berbahaya yang dapat merusak, mengganggu, atau mencuri data tanpa izin pengguna, dengan jenis-jenis seperti virus, worm, trojan, spyware, adware, dan ransomware. Penyebaran malware bisa melalui berbagai cara, termasuk email, situs web tidak aman, media penyimpanan terinfeksi, jaringan komputer, perangkat lunak tidak resmi, dan melalui teknik social engineering. Dampaknya mencakup kerusakan sistem, pencurian data, gangguan kinerja, penyebaran ke komputer lain, dan menjadi korban kejahatan seperti pada serangan

ransomware. Upaya pencegahannya melibatkan penggunaan perangkat lunak keamanan, pemahaman tentang jenis malware untuk mendeteksi infeksi, serta backup data secara rutin. Regulasi seperti UU ITE dan kerjasama antara pemerintah, lembaga terkait, dan sektor swasta turut berperan dalam menciptakan kerangka hukum yang lebih komprehensif untuk mengatasi ancaman keamanan siber. Pemahaman mendalam, upaya pencegahan, dan kerjasama lintas sektor menjadi kunci dalam melindungi sistem komputer dan data dari ancaman keamanan siber.

serangan DDoS (Distributed Denial of Service) yang bertujuan membuat layanan atau sumber daya tidak tersedia bagi pengguna yang sah. Serangan ini mengganggu ketersediaan layanan dengan membanjiri target dengan lalu lintas data berlebihan. Melalui rekrutmen botnet dan pengiriman lalu lintas berlebihan, penyerang mencoba menyumbat jaringan atau sumber daya, sulit diidentifikasi asalnya karena datang dari berbagai sumber terdistribusi di seluruh dunia.

Serangan DDoS dianggap ancaman serius karena dapat mengganggu layanan online dan berdampak pada stabilitas infrastruktur digital. Ada berbagai jenis serangan, termasuk Flood, Amplifikasi, Volumetric, dan Aplikasi, serta klasifikasi berdasarkan metode serangan di Lapisan Jaringan, Transport, dan Aplikasi. Skala dan kompleksitas serangan meningkat seiring dengan teknologi, memerlukan pembaruan strategi keamanan secara berkala.

Tujuan serangan DDoS bisa beragam, mulai dari membuat layanan tidak tersedia hingga motivasi ekonomi, politik, atau ideologi. Sumber serangan berasal dari botnets yang terdiri dari ribuan hingga jutaan perangkat terinfeksi yang dikendalikan oleh penyerang. Pendeteksian serangan DDoS memerlukan sistem pemantauan canggih, sedangkan mitigasi melibatkan konfigurasi infrastruktur yang lebih kuat, blokir lalu lintas mencurigakan, atau pengalihan lalu lintas terkena serangan. Teknologi dan layanan khusus seperti mitigasi DDoS dan scrubbing centers membantu melindungi infrastruktur dari serangan ini.

Dampak serangan DDoS meliputi penurunan ketersediaan layanan, kerusakan reputasi, dan kerugian finansial. Pencegahan termasuk penggunaan teknologi perlindungan, diversifikasi infrastruktur, pemantauan lalu lintas jaringan, perencanaan keamanan komprehensif, kebijakan keamanan yang jelas, dan pelatihan staf IT untuk mendeteksi dan mengatasi serangan DDoS.
Phishing melibatkan upaya penipuan dengan menyamar sebagai entitas tepercaya untuk memperoleh informasi pribadi atau keuangan. Metode utama termasuk pengiriman email, pesan teks, atau komunikasi online lainnya yang meniru lembaga keuangan atau perusahaan. Di sisi lain, serangan sosial menggunakan manipulasi psikologis atau interaksi sosial untuk memperoleh informasi sensitif atau merusak reputasi melalui berbagai saluran komunikasi seperti telepon, email, atau media sosial.

Perbedaan antara kedua serangan ini terletak pada pendekatan, metode, dan sasaran. Phishing cenderung memanfaatkan pesan palsu dalam komunikasi digital untuk mendapatkan informasi sensitif, sementara serangan sosial menggunakan manipulasi psikologis atau interaksi langsung untuk

mempengaruhi individu atau kelompok agar melakukan tindakan tertentu atau membagikan informasi rahasia.
Email phishing seringkali memiliki ciri-ciri tertentu, termasuk tautan mencurigakan, tekanan waktu, permintaan informasi pribadi, bahasa intimidatif, atau lampiran yang mencurigakan. Serangan phishing dan sosial dianggap serius karena dampaknya yang merugikan. Individu bisa kehilangan informasi pribadi atau keuangan yang dapat dimanfaatkan untuk pencurian identitas atau penipuan finansial. Sementara perusahaan mengalami kerusakan reputasi, kehilangan kepercayaan pelanggan, dan kerugian finansial akibat gangguan operasional atau penyalahgunaan informasi.

Serangan sosial juga dapat merusak kepercayaan personal antara individu atau mempengaruhi persepsi terhadap entitas yang dikenal. Pada tingkat perusahaan, serangan sosial dapat menyebabkan kerusakan reputasi yang serius dan mengancam keamanan informasi organisasi. Kesadaran akan risiko serangan ini serta pelatihan bagi individu dan staf perusahaan menjadi penting untuk mencegah kerugian lebih lanjut dari serangan-serangan ini.

Test Formatif 2

Pilihlah salah satu jawaban yang benar dari soal evaluasi materi berikut dengan dilingkari atau disilang.

1. Apa yang dimaksud dengan malware?
   a Perangkat keras yang tidak aman
   b Perangkat lunak yang berbahaya
   c Metode enkripsi data
   d Keamanan jaringan yang kuat

2. Serangan DDoS bertujuan untuk:
   a Mengenkripsi data penting
   b Menyebarkan virus pada sistem
   c Membuat layanan tidak tersedia bagi pengguna sah
   d Memblokir akses ke situs web yang aman

3. Bagaimana cara kerja serangan DDoS?
   a Mengirim email palsu
   b Mencuri informasi dari perangkat lain
   c Menghabiskan sumber daya sistem target dengan lalu lintas data berlebihan
   d Memperbarui keamanan perangkat lunak secara teratur

4. Jenis serangan DDoS yang mengirim lalu lintas data besar untuk menghabiskan bandwidth jaringan disebut:
   a Flood
   b Amplifikasi
   c Volumetric

d Aplikasi

5. Apa yang membuat serangan DDoS sulit diidentifikasi?
   a Karena hanya terjadi pada satu sumber
   b Karena menggunakan botnet yang terdistribusi di seluruh dunia
   c Karena sering terjadi pada jam-jam sibuk
   d Karena hanya menyerang satu jenis protokol

6. Bagaimana cara mendeteksi serangan DDoS secepat mungkin?
   a. Dengan menonaktifkan koneksi internet
   b. Dengan menggunakan sistem pemantauan yang canggih untuk memonitor lalu lintas jaringan secara terus-menerus
   c. Dengan mengubah alamat IP
   d. Dengan menghapus perangkat lunak yang tidak dikenal

7. Apa yang dimaksud dengan phishing dalam konteks keamanan siber?
   a. Mencuri informasi dengan cara meretas password
   b. Upaya memperoleh informasi sensitif dengan menyamar sebagai entitas tepercaya
   c. Menjalankan serangan pada infrastruktur jaringan
   d. Melakukan enkripsi data secara ilegal

8. Ciri-ciri email phishing yang perlu diwaspadai termasuk:
   a. Permintaan informasi pribadi, bahasa profesional, dan lampiran terbuka
   b. Tautan mencurigakan, tekanan waktu, permintaan informasi pribadi, dan bahasa yang tidak professional
   c. Bahasa intimidatif dan lampiran yang dienkripsi
   d. Permintaan informasi rahasia tanpa tekanan waktu

9. Apa tujuan utama serangan sosial dalam keamanan siber?
   a. Menghasilkan uang dari penjualan data
   b. Mencuri identitas pengguna
   c. Mendapatkan akses ke sistem secara illegal
   d. Memperoleh informasi sensitif atau merusak reputasi

10. Kenapa serangan sosial dianggap serius dalam konteks keamanan siber?
   a. Karena hanya mempengaruhi individu
   b. Karena hanya menggunakan teknologi terbaru
   c. Karena seringkali bergantung pada kelalaian atau kecerobohan manusia
   d. Karena hanya memanfaatkan kelemahan perangkat keras

Umpan Balik

Cocokan jawaban anda dengan Kunci Jawaban. Hitunglah jawaban anda yang benar, kemudian gunakan rumus di bawah ini untuk mengetahui tingkat penguasaan anda terhadapmateri Buku.

Untuk latihan soal, setiap soal memiliki bobot nilai yang sama, yaitu 10/soal.

Tes formatif:

Arti tingkat penguasaan yang Anda capai:

90 – 100 % = baik sekali

80 – 89 % = baik

70 – 79 % = cukup

< 70 % = kurang

Tindak lanjut

Bila anda mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan ke materi selanjutnya. Tetapi bila tingkat penguasaan anda masih di bawah 80%, Anda harus mengulangi materi Buku, terutama bagian yang belum anda kuasai.

MATERI

III

PROSES PENEGAKAN HUKUM DIGITAL

Indikator Keberhasilan

Setelah mempelajari Materi 2 tentang Proses Penegakan Hukum Digital ini indikator keberhasilan adalah apabila anda dapat:

- Memahami Penegak hukum yang beroperasi dalam kasus kejahatan siber, termasuk peran lembaga penegak hukum dan prosedur penyelidikan.
- Mengindentifikasi Pengumpulan bukti digital, teknik investigasi, dan proses penuntutan dalam kasus kejahatan siber (Analisis Kasus).

A. Penegak Hukum Dalam Kasus Siber

Penegakan hukum dalam kasus kejahatan siber di Indonesia melibatkan berbagai lembaga penegak hukum yang memiliki peran penting dalam mengidentifikasi, menyelidiki, menangkap, dan menuntut pelaku kejahatan yang beroperasi secara daring. Kepolisian Republik Indonesia (Polri) memiliki Direktorat Tindak Pidana Siber (Dittipidsiber) dan Bagian Reserse Kriminal Khusus (Bareskrim) yang khusus menangani kasus kejahatan siber. Mereka bertanggung jawab atas pengumpulan bukti elektronik, analisis forensik digital, dan penegakan hukum terhadap pelaku kejahatan seperti penipuan online, pencurian identitas, penyebaran malware, serta tindak kriminal lainnya yang terjadi secara daring. Selain Polri,

Kementerian Komunikasi dan Informatika (Kominfo) memiliki peran dalam pemantauan ancaman keamanan siber serta memberikan dukungan teknis pada penyelidikan kasus kejahatan siber. Sementara Badan Siber dan Sandi Negara (BSSN) bertanggung jawab dalam menjaga keamanan siber nasional dengan mendeteksi serangan, memberikan respons terhadap ancaman, dan memberikan peringatan dini terhadap potensi ancaman keamanan siber.

Prosedur penyelidikan yang dilakukan oleh lembaga penegak hukum meliputi pengumpulan bukti elektronik, analisis forensik digital untuk mengidentifikasi pelaku, serta kerja sama lintas sektor dan internasional untuk menangani kasus yang kompleks atau melintasi batas negara. Setelah terkumpul bukti yang cukup, lembaga penegak hukum melakukan penangkapan dan menuntut pelaku kejahatan siber sesuai dengan hukum yang berlaku di Indonesia. Pentingnya kolaborasi dan koordinasi antara lembaga penegak hukum seperti Polri, Kominfo, dan BSSN menjadi kunci dalam menangani kasus kejahatan siber yang semakin kompleks dan berkembang. Upaya bersama ini diperlukan untuk memastikan perlindungan terhadap warga negara dari ancaman keamanan siber serta memberikan sanksi yang sesuai terhadap pelaku kejahatan siber sesuai dengan hukum yang berlaku di Indonesia.

Tabel 6. Peran lembaga penegak hukum dan prosedur penyelidikan

ASPEK	LEMBAGA PENEGAK HUKUM	PERAN	PROSEDUR PENYELIDIKAN
Identifikasi Kasus	Direktorat Tindak Pidana Siber (Dittipidsiber) Polri	Mengidentifikasi kasus kejahatan siber	Penerimaan laporan, analisis awal, dan verifikasi informasi
	Bareskrim Polri	Menangani kasus-kasus yang kompleks dan	Pengumpulan bukti elektronik dan analisis forensik digital

		melintasi batas negara	
	Kementerian Komunikasi dan Informatika (Kominfo)	Memantau ancaman keamanan siber	Dukungan teknis pada proses penyelidikan
	Badan Siber dan Sandi Negara (BSSN)	Mempertahankan keamanan siber nasional	Pendeteksian serangan dan respons terhadap ancaman
Penyelidikan Awal	Dittipidsiber Polri	Pengumpulan bukti elektronik dan penyelidikan awal	Analisis jejak digital dan identifikasi titik awal serangan siber
	Bareskrim Polri	Menganalisis kasus-kasus yang kompleks	Pengumpulan informasi dari berbagai sumber yang relevan
	Kominfo	Pengawasan dan pemantauan atas potensi ancaman siber	Melakukan pemantauan aktif terhadap serangan dan keamanan jaringan
	BSSN	Mendeteksi ancaman dan memberikan peringatan dini	Kolaborasi dengan lembaga terkait untuk mendeteksi serangan
Kolaborasi	Dittipidsiber Polri bekerja sama dengan BSSN, Kominfo	Kolaborasi lintas lembaga dalam menangani kasus siber	Koordinasi dalam respons terhadap serangan siber yang signifikan
	Bareskrim Polri bekerja sama dengan lembaga hukum internasional	Kerja sama internasional dalam penegakan hukum	Kolaborasi dengan lembaga penegak hukum internasional dalam kasus
Penangkapan dan Penuntutan	Dittipidsiber Polri, Bareskrim Polri	Menangkap dan menuntut pelaku kejahatan siber	Penyusunan dakwaan berdasarkan bukti yang terkumpul

Table diatas memberikan gambaran mengenai peran masing-masing lembaga penegak hukum dalam penegakan hukum terkait kejahatan siber di Indonesia serta prosedur penyelidikan yang biasanya dilakukan dalam menghadapi kasus-kasus tersebut.

B. Analisis Kasus Kejahatan Siber

1. Penjelasan Kasus Putusan Nomor: 155/Pid.Sus/2018/PN-Cbn)

Dalam kasus yang dijadikan rujukan dalam Buku ini, dapat diamati dari putusan pengadilan bahwa Terdakwa didakwa oleh Penuntut Umum dengan berbagai pasal alternatif, yaitu Pasal 51 ayat (1) jo. Pasal 35, Pasal 48 ayat (1) jo. Pasal 32 ayat (1), Pasal 46 ayat (2) jo. Pasal 30 ayat (2) Undang-undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik, serta Pasal 263 Kitab Undang-Undang Hukum Pidana (KUHP) mengenai delik pemalsuan surat. Tuntutan dari pihak Penuntut Umum adalah menyatakan Terdakwa terbukti secara sah melakukan tindak pidana membuat atau memalsukan surat yang diancam oleh Pasal 263 ayat (1) KUHP, dengan ancaman pidana penjara selama 8 (delapan) bulan. Di samping itu, Penuntut Umum juga menuntut agar beberapa barang bukti yang dirampas menjadi kepunyaan Negara, serta membebankan biaya perkara kepada Terdakwa sejumlah Rp2.000, (dua ribu rupiah).

Saat berlangsungnya proses persidangan, majelis hakim melakukan pemeriksaan terhadap semua alat bukti yang dipersembahkan oleh Penuntut Umum di depan persidangan, termasuk keterangan saksi, keterangan ahli, keterangan dari Terdakwa, bukti surat, dan keterangan petunjuk. Segala hal tersebut dijadikan sebagai dasar pertimbangan untuk menilai apakah unsur-unsur delik telah terpenuhi. Hakim juga mempertimbangkan faktor-faktor yang dapat memperberat atau memperingan hukuman terhadap Terdakwa.

Pada saat Terdakwa memberikan keterangannya di persidangan, ia mengakui tidak hanya melakukan satu tindak pidana, yaitu phising, namun

juga mengakui bahwa ia melakukan tindak pidana pencurian secara elektronik (carding). Dalam putusannya, Hakim yakin dan percaya bahwa Terdakwa telah secara sah terbukti bersalah melakukan manipulasi data secara elektronik yang melanggar Undang-undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik, Pasal 51 ayat (1) jo. Pasal 35, yang berakibat pada hukuman penjara selama 8 (delapan) bulan.

Terhadap Putusan Nomor 155/Pid.Sus/2018/PN.CBN, dalam aspek hukumnya, majelis hakim telah mengambil keputusan yang sejalan dengan tuntutan yang diajukan oleh Penuntut Umum. Namun, secara menarik, berdasarkan pengakuan dan keterangan yang diberikan oleh terdakwa di hadapan persidangan, terbukti bahwa terdakwa tidak hanya terlibat dalam satu jenis tindak pidana saja, yaitu phising, melainkan juga terlibat dalam carding yang pada dasarnya merupakan tindak pencurian secara elektronik. Ini mengindikasikan bahwa terdapat lebih dari satu tindak pidana dengan unsur delik yang berbeda yang dilakukan oleh terdakwa. Dalam pandangan penulis, hal ini dapat menjadi faktor pertimbangan bagi hakim secara hukum untuk meningkatkan atau menambah hukuman terhadap terdakwa karena salah satu kriteria untuk peningkatan hukuman adalah ketika terdapat perbuatan pidana yang berbeda, di mana masing-masing perbuatan pidana tersebut dapat berdiri sendiri. Sehingga, hakim berpotensi untuk menjatuhkan hukuman dengan jumlah pidana maksimum yang paling berat ditambah sepertiga sebagaimana diatur dalam Pasal 65 ayat (2) Kitab Undang-Undang Hukum Pidana (KUHP).

Secara prinsip, menurut hukum kekuasaan kehakiman, Hakim memiliki independensi dalam menjatuhkan putusan. Artinya, Hakim diberikan

kebebasan yang sepenuhnya tanpa campur tangan dari pihak luar, baik itu berupa tekanan fisik maupun psikis saat melaksanakan tugasnya. Dengan demikian, Hakim dapat mempertimbangkan hukuman yang akan diberikan kepada Terdakwa, termasuk dalam hal pemberatan pidana, dengan memperhatikan berbagai aspek, terutama keterangan dan pengakuan Terdakwa di persidangan yang menjadi pertimbangan hukum dalam putusan.

Perlu ditekankan bahwa perbedaan antara unsur delik phising (penipuan secara elektronik) dengan carding (pencurian secara elektronik) terdapat pada Pasal yang mengaturnya. Tindak pidana phising diatur dalam Pasal 51 ayat (1) jo. Pasal 35 Undang-Undang ITE dengan ancaman hukuman maksimal 12 tahun penjara dan/atau denda maksimal 12 miliar rupiah. Sementara itu, tindak pidana carding diatur oleh Pasal 48 ayat (1) jo. Pasal 32 ayat (1) UU ITE dengan ancaman hukuman maksimal 8 tahun penjara dan/atau denda maksimal 2 miliar rupiah. Dengan demikian, setiap perbuatan pidana yang dilakukan oleh Terdakwa memiliki karakteristik tersendiri sehingga ada dasar untuk memberlakukan pemberatan pidana terhadap Terdakwa.

Dalam mengambil keputusan, Hakim tidak terikat pada tuntutan dari Penuntut Umum. Selanjutnya, jika dilihat dari besarnya kerugian yang ditimbulkan dan lamanya Terdakwa melakukan tindak pidana (sekitar 2 tahun berturut-turut sejak 2016-2018), hukuman yang diberikan kepada Terdakwa dianggap relatif rendah dengan hanya menjatuhkan hukuman 8 (delapan) bulan penjara. Hal ini karena ancaman maksimum pidana yang dapat diberikan berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Transaksi Elektronik, yaitu maksimal 12 (dua belas) tahun penjara. Selain itu, fakta di persidangan menunjukkan bahwa Terdakwa tidak hanya melakukan phising, melainkan juga carding, yaitu tindak pidana pencurian

elektronik dengan menggunakan kartu kredit milik orang lain tanpa izin untuk berbelanja online secara internasional.

2. Analisis Penerapan Sanksi Pidana Oleh Hakim

Hukuman yang diberikan kepada Terdakwa dalam kasus yang disoroti dalam tulisan ini, menurut penulis, memiliki dampak terhadap efektivitas pelaksanaan sanksi pidana yang akan dijalani oleh Terdakwa. Efektivitas pelaksanaan hukuman dapat dikaitkan dengan prinsip tujuan pemidanaan. Jika kita melihat dari sudut pandang teori tujuan pemidanaan serta tujuan dari dibentuknya Undang-Undang ITE, dapat dihubungkan dengan tercapai atau tidaknya tujuan pemidanaan tersebut.

Berdasarkan penelitian dari beberapa sumber pustaka, tujuan dari Undang-Undang Informasi dan Transaksi Elektronik yang mengancam dengan hukuman yang signifikan adalah untuk mencegah kejahatan siber dan mengurangi tingkat kejahatan, khususnya dalam ranah cyber crime terutama saat beraktivitas dan bertransaksi secara elektronik di platform sosial media dan e-commerce. Maksud dari pembentukan Undang-Undang ITE adalah untuk mencegah dan mengantisipasi penyalahgunaan teknologi informasi dan transaksi elektronik itu sendiri dengan memperhatikan nilai-nilai keagamaan dan kultural sosial masyarakat Indonesia. Sebagaimana disampaikan dalam Jurnal Kompilasi Hukum, tujuan terbentuknya UU ITE adalah untuk menghambat laju kejahatan, terutama dalam dunia maya, khususnya di media sosial. Tujuan-tujuan ini sangat terkait dengan teori tujuan pemidanaan, yang memperlakukan pemidanaan sebagai langkah pencegahan atau preventif agar tindak pidana tidak terulang atau terjadi kembali, termasuk dalam konteks kejahatan siber.

Dari tujuan-tujuan pembentukan Undang-Undang ITE yang telah diuraikan sebelumnya, dapat disimpulkan bahwa fokus utama pembentukannya adalah pada langkah-langkah preventif atau pencegahan, yang juga terkait dengan prinsip iktikad baik yang tertera dalam Pasal 3 Undang-Undang ITE. Prinsip ini digunakan oleh para pihak saat melakukan transaksi elektronik dengan maksud agar setiap individu tidak melakukan tindak pidana yang bisa berpotensi menimbulkan kerugian bagi pihak lain.

Lebih jauh lagi, teori relatif atau teori tujuan pemidanaan menjelaskan bahwa hukuman atau sanksi pidana merupakan alat untuk mencapai tujuan bersama yang bermanfaat bagi perlindungan masyarakat menuju kesejahteraan, serta untuk menjaga ketertiban hukum dalam masyarakat. Teori relatif ini memiliki tiga tujuan utama pemidanaan, yaitu preventif, detterence, dan reformatif. Pertama, tujuan preventif bertujuan untuk melindungi masyarakat dengan cara mengasingkan pelaku kejahatan dari lingkungan sosial. Kedua, tujuan detterence adalah untuk menimbulkan rasa takut pada pelaku agar mereka tidak melakukan tindak pidana. Terakhir, tujuan reformatif berusaha untuk mengubah dan memperbaiki perilaku buruk pelaku tindak pidana melalui pembinaan dan pengawasan, sehingga ketika kembali ke masyarakat, mereka dapat menjalani kehidupan sehari-hari dengan mematuhi norma-norma yang berlaku dalam masyarakat.

Jika dikaitkan dengan tujuan dibentuknya Undang-Undang ITE dan teori tujuan pemidanaan, serta terkait dengan hukuman penjara yang hanya 8 bulan bagi Terdakwa, hal tersebut berpotensi menurunkan efektivitas penerapan hukum yang telah diatur oleh pembuat undang-undang. Sebab, tujuan utama pembuat undang-undang memberikan ancaman pidana yang

tinggi pada pelanggaran Undang-Undang ITE adalah untuk mencegah agar seseorang tidak melakukan tindak pidana. Namun, jika hukuman penjara yang diputuskan oleh Hakim relatif rendah dalam lamanya, hal ini dapat mempengaruhi efektivitas tujuan pemidanaan yang diharapkan tidak tercapai.

Sebagai contoh, suatu putusan Hakim yang baik seharusnya mencakup aspek kepastian hukum, keadilan, dan kemanfaatan. Namun, jika dilihat dari putusan sebelumnya, dapat dikatakan bahwa putusan Hakim ini masih kurang memperhatikan rasa keadilan. Salah satu teori keadilan yang menguatkan argumen tersebut adalah teori keadilan korektif (remedial justice) dari Aristoteles yang bertujuan untuk memperbaiki kesalahan dalam norma-norma masyarakat dengan memberikan ganti rugi kepada pihak yang dirugikan atau memberlakukan hukuman yang sepadan.

Selain itu, teori keadilan dari Thomas Hobbes juga menguatkan argumen tersebut. Hobbes berpendapat bahwa suatu tindakan dapat dianggap adil jika berdasarkan pada perjanjian yang telah disetujui. Perjanjian tersebut tidak hanya terbatas pada kesepakatan antara dua belah pihak dalam suatu kontrak seperti jual-beli atau sewa-menyewa. Namun, juga mencakup kesepakatan dalam penjatuhan putusan antara Hakim dan terdakwa, serta peraturan hukum yang tidak memihak pada satu pihak saja, melainkan mengutamakan kepentingan umum.

Oleh karena itu, menurut penulis, hukuman penjara yang diberikan oleh Hakim dapat dikatakan belum mencapai tujuan pemidanaan dan rasa keadilan. Dengan hukuman yang relatif ringan, hal ini juga tidak mencerminkan tujuan pemidanaan dalam teori detterence (teori relatif), dimana hukuman yang seharusnya dapat menimbulkan ketakutan bagi pelaku

dan masyarakat untuk melakukan tindak pidana terutama di lingkungan sosial media. Sebaliknya, hal ini justru dapat meningkatkan pelanggaran atas aturan yang terdapat dalam Undang-Undang Informasi Transaksi Elektronik dengan memanfaatkan berbagai strategi yang mengelakkan aturan tersebut. Dengan demikian, dapat disimpulkan bahwa putusan Nomor 155/Pid.Sus/2018/PN-Cbn belum sepenuhnya sesuai dengan tujuan pemidanaan yang diinginkan dan belum memenuhi prinsip keadilan.

Latihan Soal 3

1. Tantangan dan Peran Lembaga Penegak Hukum dalam Kasus Kejahatan Siber Dalam konteks kompleksitas kasus kejahatan siber, jelaskan tantangan utama yang dihadapi oleh lembaga penegak hukum seperti Polri, Kominfo, dan BSSN dalam upaya mengidentifikasi, menyelidiki, dan menuntut pelaku kejahatan siber di Indonesia. Jelaskan peran serta pentingnya kolaborasi di antara lembaga-lembaga tersebut dalam menangani ancaman keamanan siber yang terus berkembang di era digital saat ini.
2. Kerjasama Lintas Sektor dan Penanganan Kasus Kejahatan Siber di Indonesia Gambarkan langkah-langkah konkret yang dilakukan oleh lembaga penegak hukum seperti Polri, Kominfo, dan BSSN dalam kerjasama lintas sektor dan internasional dalam menangani kasus kejahatan siber yang melintasi batas negara. Jelaskan pentingnya koordinasi antarlembaga tersebut dalam proses penyelidikan, pengumpulan bukti, analisis forensik digital, serta penegakan hukum

terhadap pelaku kejahatan siber yang semakin kompleks dan berkembang di Indonesia.

3. Buatlah rangkuman dari apa yang sudah Anda pelajari dari Studi Kasus Proses Penegakan Hukum Digital!

Apabila belum berhasil menjawab silahkan pelajari kembali materi terkait Proses Penegakan Hukum Digital. Selamat berlatih.

Rangkuman

Proses penegakan hukum digital di Indonesia merupakan rangkaian upaya yang dilakukan oleh pemerintah dan lembaga terkait untuk mengawasi, menindak, serta mengatasi pelanggaran hukum yang terjadi di ruang digital. Keberadaan teknologi informasi dan komunikasi yang semakin merajalela memunculkan berbagai tantangan hukum yang perlu ditangani dengan cermat. Upaya penegakan hukum digital di Indonesia telah mengalami evolusi sejalan dengan perkembangan teknologi. Peraturan perundang-undangan, khususnya Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), menjadi dasar dalam menegakkan hukum di ranah digital. UU ITE mengatur sejumlah kejahatan digital seperti penyebaran informasi bohong, pencemaran nama baik, penipuan, serta tindak pidana lain yang melibatkan penggunaan teknologi digital. Meski demikian, peran serta lembaga penegak hukum seperti Kepolisian, Kejaksaan, dan Badan Siber dan Sandi Negara (BSSN) memegang peran krusial dalam memastikan implementasi hukum digital.

Tantangan dalam penegakan hukum digital meliputi beragam hal, seperti

kesulitan dalam menentukan yurisdiksi atas kasus-kasus yang melintasi batas wilayah maya, kecepatan perkembangan teknologi yang dapat dimanfaatkan untuk kejahatan, serta perlindungan terhadap data pribadi dan privasi pengguna. Perlindungan data pribadi menjadi isu yang semakin mendesak dalam konteks penegakan hukum digital. Berbagai regulasi, seperti Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) No. 20 Tahun 2016, ditetapkan untuk melindungi data pribadi dan menetapkan kewajiban bagi pemilik data serta pengelola data.

Pemerintah Indonesia terus berupaya memperkuat penegakan hukum digital melalui berbagai langkah. Hal ini meliputi peningkatan kapasitas lembaga penegak hukum dalam menghadapi tantangan teknologi, peningkatan kesadaran masyarakat terhadap aspek hukum digital, serta kerjasama internasional untuk menangani kejahatan digital yang melintasi batas negara. Implikasi dari penegakan hukum digital tidak hanya berkaitan dengan keamanan dan perlindungan data, tetapi juga memiliki dampak sosial dan ekonomi yang signifikan. Upaya ini bukan hanya untuk menjaga keamanan digital, tetapi juga untuk memelihara kepercayaan masyarakat terhadap teknologi digital, meningkatkan efisiensi bisnis di era digital, dan mendukung pertumbuhan ekonomi yang berkelanjutan.

Dalam konteks yang semakin kompleks ini, upaya penegakan hukum digital menjadi semakin penting. Perlindungan data dan privasi, peningkatan kapasitas lembaga penegak hukum, serta kesadaran akan tata kelola digital menjadi poin kunci dalam menjaga keamanan dan kepercayaan masyarakat terhadap teknologi. Seiring dengan perubahan teknologi yang pesat, penegakan hukum digital akan terus berkembang guna menjawab

tantangan baru yang muncul di ranah digital, dan hal ini menjadi bagian integral dalam upaya menciptakan lingkungan digital yang aman, adil, dan terpercaya.

Tes Formatif 3

1. Organisasi yang bertanggung jawab atas pengumpulan bukti elektronik, analisis forensik digital, dan penegakan hukum terhadap kejahatan siber di Indonesia adalah:
   a) Kementerian Pertahanan
   b) Polri
   c) Kementerian Kesehatan
   d) Kementerian Keuangan
2. Lembaga yang memiliki Direktorat Tindak Pidana Siber (Dittipidsiber) dan Bagian Reserse Kriminal Khusus (Bareskrim) yang khusus menangani kasus kejahatan siber adalah:
   a) Kementerian Komunikasi dan Informatika (Kominfo)
   b) Badan Siber dan Sandi Negara (BSSN)
   c) Kepolisian Republik Indonesia (Polri)
   d) Badan Intelijen Negara (BIN)
3. Tugas utama Badan Siber dan Sandi Negara (BSSN) adalah:
   a) Memberikan respons terhadap ancaman keamanan siber
   b) Analisis forensik digital
   c) Pengumpulan bukti elektronik
   d) Penyelidikan kasus kejahatan siber
4. Langkah pertama dalam prosedur penyelidikan kejahatan siber adalah:
   a) Analisis forensik digital
   b) Penangkapan pelaku
   c) Pengumpulan bukti elektronik
   d) Kerja sama lintas sektor dan internasional
5. Tindakan yang dilakukan setelah terkumpul bukti yang cukup dalam penyelidikan kejahatan siber adalah:
   a) Penangkapan dan penuntutan pelaku sesuai hukum yang berlaku
   b) Analisis forensik digital
   c) Pengumpulan bukti elektronik
   d) Pemantauan ancaman keamanan siber

Umpan Balik

Cocokan jawaban anda dengan Kunci Jawaban. Hitunglah jawaban anda yang benar, kemudian gunakan rumus di bawah ini untuk mengetahui tingkat penguasaan anda terhadapmateri Buku.

Untuk latihan soal, setiap soal memiliki bobot nilai yang sama, yaitu 20/soal.

Tes formatif:

Arti tingkat penguasaan yang Anda capai:

90 – 100 % = baik sekali

80 – 89 % = baik

70 – 79 % = cukup

< 70 % = kurang

Tindak lanjut

Bila anda mencapai tingkat penguasaan 80% atau lebih, Anda dapat meneruskan ke materi selanjutnya. Tetapi bila tingkat penguasaan anda masih di bawah 80%, Anda harus mengulangi materi Buku, terutama bagian yang belum anda kuasai.

PENUTUP

Buku Hukum Digital Security adalah suatu panduan yang mencakup berbagai aspek penting yang mengatur dan melindungi lingkungan digital dalam konteks hukum. Dalam era di mana teknologi digital semakin merajalela, pemahaman mendalam tentang kerangka hukum yang mengatur keamanan digital menjadi esensial bagi individu maupun organisasi. Melalui pemahaman tentang hak privasi, hukum cipta, kekayaan intelektual, peraturan kontrak elektronik, dan hukum komunikasi elektronik, Buku ini memberikan wawasan yang komprehensif tentang upaya perlindungan terhadap data dan sistem dalam dunia yang terus berkembang ini.

Buku ini menggali implikasi hukum yang timbul dari pelanggaran data pribadi dan keamanan siber, menggarisbawahi konsekuensi serius yang dapat menghantui individu atau entitas yang melanggar peraturan tersebut. Pelanggaran dapat mengakibatkan sanksi yang berat, termasuk denda besar, tuntutan ganti rugi, hukuman pidana, dan kerugian reputasi. Oleh karena itu, pentingnya kepatuhan terhadap undang-undang privasi dan keamanan siber tidak bisa diabaikan.

Dengan menjelaskan konsep-konsep dasar seperti kerentanan, ancaman, risiko, serta prinsip-prinsip pertahanan dalam kedalaman dan privasi by design, Buku ini bertujuan memberikan pemahaman yang mendalam tentang bagaimana melindungi data dan sistem dari berbagai ancaman keamanan dalam lingkungan digital yang selalu berubah.

Kesimpulannya, Buku ini merupakan panduan yang sangat berguna untuk semua pihak yang ingin memahami, mengikuti, dan mematuhi regulasi-regulasi hukum yang berkaitan dengan keamanan digital, guna melindungi hak individu dan organisasi, serta mencegah konsekuensi hukum yang merugikan.

KUNCI JAWABAN

Jawaban Tes Formatif 1

3. B. Hak individu terhadap privasi dalam dunia digital
4. B. Hak atas kekayaan intelektual dalam konten digital
5. A. Validitas dan penegakan kontrak yang dibuat secara elektronik
6. A. Hak individu terhadap privasi dalam dunia digital
7. A. Menjaga informasi agar tidak bocor kepada pihak yang tidak berkepentingan
8. D. Sanksi finansial dan perdata, tergantung pada tingkat pelanggaran dan yurisdiksi hukum yang berlaku.
9. C. Undang-undang yang mengatur tindakan kriminal dalam keamanan siber dan penting untuk penyelidikan dan penuntutan pelaku.
10. C. Regulasi Perlindungan Data Umum (GDPR)
11. C. Hukuman penjara
12. C. Untuk memahami bagaimana melindungi sistem dan data dalam lingkungan digital

Jawaban Tes Formatif 2

1. B. Perangkat lunak yang berbahaya
2. Membuat layanan tidak tersedia bagi pengguna sah
3. Menghabiskan sumber daya sistem target dengan lalu lintas data berlebihan
4. C. Volumetric
5. B. Karena menggunakan botnet yang terdistribusi di seluruh dunia
6. B. Dengan menggunakan sistem pemantauan yang canggih untuk memonitor lalu lintas jaringan secara terus-menerus
7. B. Upaya memperoleh informasi sensitif dengan menyamar sebagai entitas tepercaya
8. B. Tautan mencurigakan, tekanan waktu, permintaan informasi pribadi, dan bahasa yang tidak profesional
9. Memperoleh informasi sensitif atau merusak reputasi
10. C. Karena seringkali bergantung pada kelalaian atau kecerobohan manusia

Jawaban Tes Formatis 3

1. A. Polri
2. C. Kepolisian Republik Indonesia (Polri)
3. A. Memberikan respons terhadap ancaman keamanan siber
4. C. Pengumpulan bukti elektronik
5. A. Penangkapan dan penuntutan pelaku sesuai hukum yang berlaku

DAFTAR PUSTAKA

BUKU REFRENSI

Gani, Taufiq A. *Kedaulatan Data Digital untuk Integritas Bangsa*. Syiah Kuala University Press, 2023.

Wibowo, Arief, Yehu Wangsajaya, and Asep Surahmat. *Pemolisian Digital dengan Artificial Intelligence*. PT. Raja Grafindo Persada-Rajawali Pers, 2023.

Dahlan Sinaga SH, M. H. *Sejarah Pluralitas Hukum dan Hukum Pidana di Indonesia: Seri Penegakan Hukum*. Nusamedia, 2021.

Aris Hardinanto, 2019, *Akses Ilegal dalam Perspektif Hukum Pidana*, Malang: Setara Press

Eko Budi, 2019, *Hukum Tindak Pidana Khusus*, CV. Pena Persada, Jawa Tengah

Abdul Wahid dan Mohammad Labib, 2005, *Kejahatan Mayantara*, PT Refika Aditama, Bandung

Effendi, Basri. "*Pengawasan Dan Penegakan Hukum Terhadap Bisnis Digital (E-Commerce) Oleh Komisi Pengawas Persaingan Usaha (KPPU) Dalam Praktek Persaingan Usaha Tidak Sehat*." Syiah Kuala Law Journal 4.1 (2020): 21-32.

Chotimah, Hidayat Chusnul. "*Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]."* Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional 10.2 (2019): 113-128.

Rahmawati, Cynthia. "*Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0.*" Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia (SENASTINDO). Vol. 2. 2020.

PERUNDANG-UNDANGAN

Kitab Undang-Undang Hukum Pidana

Undang-Undang Dasar Negara Republik Indonesia 1945

Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan

Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan

Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 20 Tahun

2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik.

WEB INTERNET

Abdul Muslim, 2022, “Kuartal I-2022, Ada lebih dari 3000 Serangan Phising di

Indonesia”, Investor Daily, (Ceted 2022 Des. 26), availble from:

https://investor.id/it-and-telecommunication/288425/kuartal-i2022-adalebih-dari-3000-serangan-phising-di-indonesia

GLOSARI

Cybercrime	: Kejahatan yang dilakukan dengan menggunakan teknologi informasi dan komunikasi, seperti peretasan, pencurian identitas, pencurian data, dan kejahatan lain yang terkait dengan teknologi.
Data Protection Laws	: Undang-undang yang mengatur pengumpulan, penggunaan, penyimpanan, dan keamanan informasi pribadi individu atau organisasi untuk melindungi data dari penyalahgunaan atau pelanggaran keamanan.
Digital Forensics	: Proses investigasi dan analisis terhadap bukti digital yang digunakan dalam pengungkapan kejahatan, peretasan, atau insiden keamanan lainnya.
Encryption Laws	: Peraturan atau kebijakan yang mengatur penggunaan enkripsi untuk melindungi data pribadi atau rahasia dalam konteks hukum.
Legal Hold	: Proses di mana data atau informasi elektronik diidentifikasi, disimpan, dan dilindungi sebagai bagian dari proses hukum, terutama dalam kasus litigasi.
Privacy Laws	: Peraturan atau undang-undang yang mengatur bagaimana informasi pribadi individu atau entitas harus diperlakukan, disimpan, dan diakses dalam konteks digital untuk melindungi privasi.
Risk Assessment	: Evaluasi yang dilakukan untuk mengidentifikasi, mengevaluasi, dan mengelola potensi ancaman atau risiko terhadap keamanan data dan sistem komputer.
Security Incident	: Kejadian yang mengancam atau mengganggu keamanan sistem informasi atau data, termasuk serangan, insiden kehilangan data, atau peretasan.
Digital Evidence	: Informasi atau bukti elektronik yang digunakan dalam konteks hukum, seperti email, file komputer, log aktivitas, atau data forensik yang digunakan dalam penyelidikan dan proses pengadilan.

Penerbit : UNPRI PRESS