PENGABDIAN MASYARAKAT :

MENINGKATKAN KESADARAN MASYARAKAT TERHADAP KEJAHATAN CYBERCRIME PADA M.BANKING KEPADA RUKUN WARGA 9 KELURAHAN KWITANG KECAMATAN SENEN

OLEH :

Amas Sari Marthanti, S.E., M.M. **(201809123)**

Jaka Santosa, S.H., M.H. **(200109627)**

Hartana, ST., M.T. **(202003046)**

Dra. Maria Lapriska Dian Ela Revita, M.M. **(201209463)**

UNIVERSITAS BINA SARANA INFORMATIKA

1 Nopember 2024

Pendahuluan

Beberapa waktu lalu media sosial digemparkan oleh **kasus hilangnya uang seorang *netizen* dari *mobile banking***, setelah **mengunduh *file* dengan ekstensi .apk** dari seseorang yang mengaku sebagai **kurir *e-commerce***. **Kasus pencurian data merupakan salah satu jenis kasus *cyber crime* yang saat ini sering terjadi**. Seiring dengan perkembangan teknologi komputer dan internet, berkembang pula cara pelaku kriminal untuk mencuri data perusahaan maupun individu. Banyaknya pengguna teknologi maka semakin banyak kejahatan atau Cyber crime. **Salah satu kejahatan *cyber crime* yaitu *malware*.**

Malware merupakan perangkat lunak yang bekerja dengan memasuki komputer tanpa perizinan serta dapat menyebabkan kerusakan pada sistem, server, dan jaringan komputer. Malware merupakan gabungan dari kata malicious yang berarti jahat atau berbahaya dan software yang berarti perangkat lunak, dapat melakukan pencurian data dan informasi yang tersimpan dalam komputer serta menjadi pintu belakang masuknya hacker, yang masuk pada sistem komputer dengan melalui jaringan internet. Pada umumnya, perangkat lunak ini **disisipkan pada unduhan pada situs web ilegal, iklan, email phishing**, dan lain lain. **Malware diciptakan** oleh **para hacker** yang memiliki pemahaman tinggi akan perangkat lunak dengan tujuan tertentu.

UNIVERSITAS
BINA SARANA INFORMATIKA

Pendahuluan

Menurut data yang dikumpulkan oleh **comparitech.com**, terdapat 153 juta *malware* baru pada tahun 2021 dan 93,6% di antaranya mampu merubah kode penyusunnya, sehingga susah untuk dideteksi. Selain itu, lebih dari 50% komputer yang sudah pernah terkena peretasan, berpeluang untuk terkena peretasan lagi pada tahun yang sama. `

Penting untuk diingat, dalam menggunakan internet selalu waspada pada iklan, link, promosi, dan website. Apabila sebuah situs terlihat mencurigakan, hindari mengklik konten yang tersedia di dalamnya, bisa saja malware masuk ke komputer melalui situs tersebut.

Maka dari itu, tidak heran jika saat ini pengamanan siber data-data bisnis harus dijaga dengan teknologi terbaru. Maka perlu merumuskan teknologi apa yang cocok untuk mengamankan data-data Perusahaan
`

UNIVERSITAS
BINA SARANA INFORMATIKA

https://www.linknet.id/article/cyber-crime

Cyber Crime ?

Pengertian : ***Cyber crime*** **atau kejahatan cyber adalah tindak kejahatan yang memanfaatkan teknologi komputer dan jaringan internet untuk melakukan peretasan, pencurian, penipuan, penyebaran *virus*, dan tindak kriminal digital lainnya.**

Kejahatan cyber merupakan tindakan kejahatan yang berkaitan dengan komputer maupun perangkat jaringan, biasanya kejahatan ini dilakukan secara online. bahkan kejahatan cyber ini bisa menargetkan siapa saja, hal ini tentu akan mengakibatkan banyak kerugian bagi korbannya. Kejahatan siber sering terjadi karena adanya kerentanan atau celah dalam sistem keamanan. Apalagi tak semua orang menjadikan keamanan sebagai prioritas. Bahkan ada juga yang mengabaikan sistem keamanan dan tidak memperbaharuinya

UNIVERSITAS
BINA SARANA INFORMATIKA

Landasan Hukum Cyber Crime ?

Hukum Indonesia yang mengatur cybercrime :
Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE),

Bagian mengatur yurisdiksi yang bagian ke-2 mencakup dasar teritorial subjektif bagi setiap orang melakukan cybercrime dan dikualifikasi berbahaya di Indonesia .

Indonesia telah mempunyai peraturan untuk mencegah terjadinya cyber crime yang lebih dikenal dengan sebutan : **Cyber Law.**
Cyber Law akan menjadi dasar hukum dalam proses penegakan hukum terhadap kejahatan-kejahatan dengan sarana elektronik dan komputer, termasuk kejahatan pencucian uang dan kejahatan terorisme. Dengan kata lain, Cyber Law diperlukan untuk menanggulangi kejahatan Cyber.

UNIVERSITAS
BINA SARANA INFORMATIKA

Dampak Cyber Crime ?

Dampak terbesar akibat cyber crime, khususnya peretasan data perusahaan adalah **penurunan kepercayaan masyarakat** terhadap perusahaan tersebut. Apabila kepercayaan masyarakat menurun, bukan tidak mungkin mereka akan melakukan aksi tambahan, seperti **menghapus aplikasi** dari handphone mereka, atau **berhenti berlangganan produk dan jasa** yang dihasilkan oleh perusahaan tersebut.

Menurut **hasil penelitian** yang dilakukan oleh Kaspersky sebagaimana diberitakan oleh Liputan6.com, sebanyak **29% perusahaan** yang menjadi objek penelitian lembaga tersebut, **mengalami kesusahan untuk mendapatkan pelanggan baru** pasca sistemnya diretas. Pada akhirnya, **pendapatan perusahaan** akan **mengalami penurunan.**

UNIVERSITAS
BINA SARANA INFORMATIKA

Jenis Cyber Crime ?

1. *Phishing*

Phishing adalah tindakan penipuan *online* yang bertujuan untuk memancing Anda untuk membocorkan data-data pribadi, seperti nomor kartu kredit, kode OTP dan lain sebagainya. Pelaku tindak kejahatan ini biasanya menggunakan situs palsu yang menyerupai sebuah institusi untuk mencuri identitas Anda.
Contoh :
pelaku mengirim email yang seolah menginginkan perusahaan yang dipimpin menjadi mitra. Dalam email tersebut, pengirim mencantumkan tautan. Jika Perusahaan, mengklik tautan tersebut dan mengisi informasi sensitif di halaman tersebut, maka data sensitif perusahaan akan tercuri.

UNIVERSITAS
BINA SARANA INFORMATIKA

2. Serangan Ransomware

Ransomware adalah jenis *malware* yang dapat menyerang gawai seseorang dan membuat orang tersebut tidak bisa mengakses gawainya sampai dia membayar sejumlah uang yang diinginkan oleh pengirim *malware* tersebut. Tentu hal ini sangat merugikan pengguna internet, sebab ini artinya data-data penting yang mereka simpan di gawai tersebut terancam hilang atau diperjualbelikan.

Bayangkan jika laptop perusahaan terkena *ransomware* dan data bisnis tidak bisa diakses sebelum perusahaan membayar sejumlah uang. Sangat merepotkan perusahaan, sehingga perlu diantisipasi segera.

BINA SARANA INFORMATIKA
UNIVERSITAS
BINA
SARANA
INFORMATIKA

3. Carding

Carding adalah kejahatan siber yang memanfaatkan data kartu kredit orang lain untuk bertransaksi. Data kartu kredit tersebut dapat diperoleh dengan berbagai cara, misalnya meretas situs tempat Anda menggunakan nomor kartu kredit untuk berlangganan dan menanamkan *hardware* khusus di balik mesin EDC yang Anda gunakan untuk membayar di supermarket. *Hardware* khusus ini digunakan untuk merekam data kartu yang telah Anda gesek dan mengirimkannya kepada oknum penipu terkait.

UNIVERSITAS
BINA SARANA INFORMATIKA

4. Cracking

Cracking adalah sebuah tindak kejahatan berupa *cyber intrusion* yang dilakukan dengan masuk ke dalam sistem sebuah komputer atau *software* dengan cara menghapus sistem keamanan *software* atau komputer tersebut. Tujuan dari *cracker* atau pelaku tindak pidana *cracking* ada berbagai macam, mulai dari menanamkan *malware*, mencuri data, hingga membuat software bajakan. *Cracking* mirip dengan *hacking*. Bedanya, tidak semua kegiatan *hacking* bertujuan buruk. Ada banyak *hacker* yang menggunakan keahliannya untuk menilai sistem keamanan sebuah situs dan memberitahunya kepada pemilik situs tersebut, seperti melakukan *penetration testing*.

UNIVERSITAS
BINA SARANA INFORMATIKA

5. OTP Fraud

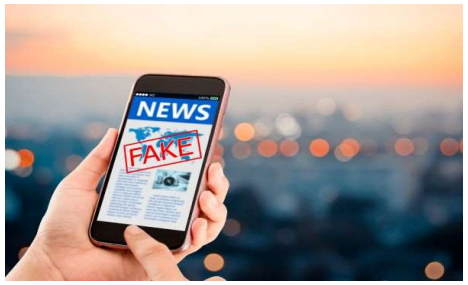
One-time password atau OTP adalah serangkaian kode sekali pakai yang dikirimkan oleh sistem ke nomor handphone atau email yang terdaftar di sistem tersebut. Tujuan dari pengiriman kode OTP ini adalah untuk pengamanan ganda. Namun sayangnya, saat ini banyak juga penipu yang menggunakan kode ini untuk melakukan tindak kejahatan. Modusnya adalah Ketika akan dihubungi oleh penipu melalui WhatsApp atau telepon dengan mengaku dari pihak bank. Penipu lantas mengatakan kalau kartu Anda sedang mengalami masalah dan menawarkan bantuan. Salah satu syarat bantuan tersebut adalah menyebutkan kode OTP palsu yang dikirimkan ke nomor handphone atau email korban. Jika korban menyebutkan kode tersebut, maka bisa jadi aplikasi mobile bankingnya tidak bisa digunakan lagi atau saldonya habis.

UNIVERSITAS
BINA SARANA INFORMATIKA

6. *Cyberbullying*

Media yang digunakan untuk melakukan *cyber crime* tidak hanya media dengan teknologi tinggi. Salah satu jenis kejahatan siber yang bisa dilakukan oleh siapapun dengan gawai apapun dan tetap berbahaya adalah *cyberbullying* atau perundungan *online.* Bahkan, tidak jarang akibat perundungan oleh *netizen*, seseorang bisa mengakhiri hidupnya sendiri.

7. Kejahatan Konten



Cyber crime juga melingkupi kejahatan yang melibatkan konten, mulai dari plagiasi konten hingga sengaja menjiplak *website* atau menyebarkan informasi-informasi tidak benar (*hoax*) di internet.

UNIVERSITAS

BINA
SARANA
INFORMATIKA

Kejahatan Cyber Crime ?

Contoh Kasus *Cyber Crime* di Indonesia

Salah satu contoh kasus cyber crime yang sempat ramai diperbincangkan pa tahun 2020 lalu adalah kasus bocornya 91 juta data pengguna Tokopedia. Kasus diawali dengan cuitan akun @underthebreach di Twitter yang mengkla bahwasanya 91 juta data pengguna aplikasi e-commerce tersebut sedang dijual black market bernama RaidForums.

Adapun data yang diperjualbelikan tersebut adalah User ID, email, nama lengkap, tanggal lahir, jenis kelamin, nomor handphone dan password dari pengguna aplikasi tersebut. Tak pelak hal ini berakibat pada penurunan kepercayaan masyarakat terhadap aplikasi tersebut.

UNIVERSITAS
BINA SARANA INFORMATIKA

Mencegah dan Mengatasi Cyber Crime

1. Mengedukasi masyarakat mengenai tata cara pencegahan *cyber crime*.
2. Tidak memencet sembarang *link* atau tautan.
3. Memperbaharui password secara berkala.
4. Memasang perangkat lunak antivirus, anti *malware* dan sejenisnya di gawai komputer
5. Menggunakan *secure socket layer* (SSL) untuk tambahan keamanan pada situs yang dimiliki

BINA SARANA INFORMATIKA
UNIVERSITAS
BINA
SARANA
INFORMATIKA

Cyber Security ?

Cyber security : bentuk perlindungan terhadap sistem yang terhubung ke internet. Ini termasuk perangkat keras, perangkat lunak hingga data yang dimiliki.

Praktik *cyber security* dilakukan tidak hanya oleh individu, tapi juga oleh perusahaan dan instansi. Langkah ini akan membantu melindungi pusat data dan sistem komputerisasi lainnya dari akses yang tidak sah.

Strategi keamanan siber yang mumpuni bisa memberikan perlindungan keamanan yang baik terhadap serangan yang dirancang untuk mengakses, mengubah, menghapus atau memeras sistem dan data sensitif dari pengguna.

Keamanan cyber juga berperan dalam mencegah serangan yang bertujuan untuk mengganggu atau bahkan menghentikan operasi sistem maupun perangkat.

UNIVERSITAS
BINA
SARANA
INFORMATIKA

m-Banking ?

Mobile Banking: biasa disingkat dengan m-Banking, merupakan transaksi perbankan melalui media handphone baik dalam bentuk aplikasi m-Banking atau aplikasi bawaan operator seluler.

Keuntungan memanfaatkan m-Banking

1. Praktis , tidak perlu membawa dan menghitung uang tunai
2. Aman, menggunakan PIN/ kode rahasia

Layanan m-Banking ?

1. Transfer dana;
2. Informasi saldo;
3. Mutasi rekening;
4. Informasi nilai tukar;
5. Pembayaran (kartu kredit,PLN,telepon,handphone,listrik,asuransi);
6. Pembelian (pulsa isi ulang, saham).

UNIVERSITAS
BINA SARANA INFORMATIKA

Modus Kejahatan Cyber Crime pada M-Banking

1. Pharming :
Penipu atau *hacker* melakukan pengalihan dari situs yang sah ke situs palsu tanpa diketahui dan disadari oleh korban. Kemudian mengambil data yang dimasukkan oleh korban sehingga masuk ke dalam area yang menjadi permainan penipu tersebut.

2. Spoofing :
Menggunakan perangkat lunak untuk menutupi identitas dengan menampilkan alamat e-mail/ nama/ nomor telepon palsu di komputer agar menyembunyikan identitas. Untuk melakukan penipuan mereka menimbulkan kesan berurusan dengan pebisnis terkemuka.

3. Keylogger :
Software yang dapat menghafal tombol *keyboard* yang digunakan tanpa diketahui oleh pengguna.

UNIVERSITAS
BINA SARANA INFORMATIKA

Modus Kejahatan Cyber Crime pada M-Banking

4. Phising. :

Tindakan memperoleh informasi pribadi seperti user ID, PIN, nomor rekening bank/ nomor kartu kredit secara tidak sah. Informasi ini kemudian dimanfaatkan untuk mengakses rekening, melakukan penipuan kartu kredit atau memandu nasabah untuk melakukan transfer ke rekening tertentu dengan iming-iming hadiah.

5. Sniffing :

Pekerjaan menyadap paket data yang lalu-lalang pada jaringan.

BINA SARANA INFORMATIKA UNIVERSITAS

Penanggulangan Kejahatan Cyber Crime pada M-Banking?

1. Lindungi komputer nasabah dengan perangkat lunak *anti-virus, spyware filter, filter e-mail* dan *program firewall*.

2. Segera hubungi Bank yang bersangkutan dan laporkan kecurigaan nasabah

3. Jangan membalas *e-mail* yang meminta informasi pribadi. Bank tidak pernah meminta informasi pribadi seperti PIN atau *password*.

4. Pastikan akses alamat *website internet banking* nasabah yang benar. Jangan klik dengan kata yang sengaja disalahejakan atau mirip dengan yang asli.

UNIVERSITAS
BINA SARANA INFORMATIKA

Akibat Kejahatan Cyber Crime pada M-Banking

Penggunaan media internet dewasa ini tidak dapat dipisahkan dalam kehidupan sehari-hari. Salah satunya di industri jasa keuangan yakni sektor perbankan yang mengeluarkan layanan *internet banking* dan *mobile banking* yang memudahkan nasabah untuk melakukan kegiatan perbankan seperti transfer dana, informasi saldo, mutasi rekening, informasi nilai tukar, pembayaran (kartu kredit, rekening listrik, rekening telepon, asuransi), dan pembelian (pulsa isi ulang, saham).

Namun, layanan tersebut memiliki celah untuk dilakukannya kejahatan yang dilakukan oleh penjahat yang memiliki keahlian dalam penggunaan sistem atau yang sering disebut *(Cyber Crimer).* Bagi *Cyber Crimer*, kejahatan melalui *internet banking/ mobile banking* dapat menjangkau jutaan calon korban dengan biaya yang tidak mahal. Kejahatan *internet banking/ mobile banking* ini telah merugikan banyak pengguna dan terus mengalami peningkatan.

UNIVERSITAS
BINA SARANA INFORMATIKA

Faktor yang mempengaruhi Kesadaran Masyarakat pengguna M-Banking terhadap ancaman Cybercrime ?

1. **sosiodemografi,** yang terdiri dari usia, jenis kelamin, tingkat pendidikan, dan pekerjaan dapat mempengaruhi kesadaran dan pemahaman seseorang terhadap ancaman cybercrime

2. **tingkat penggunaan mobile banking**

Frekuensi dan intensitas penggunaan mobile banking dapat berpengaruh. Pengguna yang lebih sering menggunakan layanan ini akan lebih sadar akan praktik keamanan yang diperlukan

3. **kepuasan terhadap keamanan mobile banking**, kepuasan pengguna terhadap fitur keamanan yang disediakan oleh bank dapat mencerminkan kesadaran mereka terhadap pentingnya perlindungan data pribadi dan transaksi finansial

4. **persepsi risiko,** yang merupakan persepsi individu mengenai risiko yang terkait dengan penggunaan mobile banking sangat penting dalam menentukan tingkat kewaspadaan mereka terhadap ancaman cybercrime. Pengguna yang merasa bahwa risiko cybercrimetinggi cenderung lebih berhati-hati dalam menggunakan layanan ini

UNIVERSITAS
BINA SARANA INFORMATIKA

Faktor yang mempengaruhi Kesadaran Masyarakat pengguna M-Banking terhadap ancaman Cybercrime ?

5. **Pengalaman pribadi nasabah**. Pengalaman pribadi dengan insiden keamanan, seperti penipuan atau pelanggaran data, dapat meningkatkan kesadaran dan pengetahuan pengguna tentang ancaman cybercrime dan langkah-langkah yang perlu diambil untuk mencegahnya.

6. **Kepatuhan pengguna terhadap praktik keamanan yang direkomendasikan**, seperti penggunaan kata sandi yang kuat dan otentikasi dua faktor, merupakan indikator penting dari kesadaran mereka terhadap ancaman cybercrime

7. K**esiapan nasabah** dalam menghadapi ancaman cybercrime. Kesiapan dan kemampuan pengguna dalam menghadapi ancaman, seperti pengetahuan tentang cara melaporkan insiden keamanan dan mengatasi serangan siber, menunjukkan tingkat kesadaran yang lebih tinggi

8**. Tingkat pengetahuan pengguna tentang cybercrime**. Pengetahuan umum pengguna tentang jenis-jenis cybercrimedan metode perlindungan adalah kunci dalam menilai kesadaran mereka terhadap ancaman ini. Pendidikan dan informasi yang tepat dapat meningkatkan tingkat pengetahuan dan kesadaran pengguna

UNIVERSITAS
BINA SARANA INFORMATIKA

Daftar Pustaka

https://www.linknet.id/article/cyber-crime

Junedi Hutagaol, Riama Santy Sitorus, Nindya HutagaolIdentifikasi Tingkat Kesadaran Pengguna Mobile Banking terhadap Ancaman Cybercrime
Jurnal Teknologi Sistem Informasi dan AplikasiISSN: 2654-3788Penerbit: Program Studi Teknik Informatika Universitas Pamulange-ISSN: 2654-4229Vol. 7, No. 3, http://openjournal.unpam.ac.id/index.php/JTSI1043

BINA SARANA INFORMATIKA
UNIVERSITAS
BINA
SARANA
INFORMATIKA

TERIMA - KASIH

UNIVERSITAS
BINA
SARANA
INFORMATIKA