Jurnal ABDIMAS-IBISA
Pengabdian Kepada Masyarakat

Vol.1 No.2
Juni 2023
Hal : 34 – 41

MANAJEMEN INSIDEN KEAMANAN CYBER SECURITY PEMERINTAHAN INDONESIA AGAR TERCIPTANYA KEAMANAN TRANSAKSI E-COMMERCE DI INDONESIA

Rizki Dewantara, S.Kom., M.Kom[1]

Program Studi S1 Sains Data, Fakultas Sains Teknologi dan Kesehatan,

Institut Teknologi Bisnis Dan Kesehatan Bhakti Putra Bangsa Indonesia

Email: dewantararizki@ibisa.ac.id

Jl. Soekarno Hatta Borokulon Banyuurip Purworejo

Nadifa Gita Salsabila[2]

Program Studi Informatika, Universitas Perwira Purbalingga, Indonesia

Email: yuukinadifa@gmail.com

Jl. Letjen S Parman No.53, Kedung Menjangan, Kec. Purbalingga, Kabupaten Purbalingga, Jawa Tengah

Windi Amilina Asiska[3]

Program Studi S1 Sains Data, Fakultas Sains Teknologi dan Kesehatan,

Institut Teknologi Bisnis Dan Kesehatan Bhakti Putra Bangsa Indonesia

Email: windiamiliaa0404@gmail.com

Jl. Soekarno Hatta Borokulon Banyuurip Purworejo

ABSTRAK

Teknologi informasi terus berinovasi dan bertransformasi menjadi semakin canggih. Dengan kecanggihannya teknologi ini dapat memberikan banyak kemudahan bagi kehidupan masyarakat, diantaranya yaitu dengan menggunakan teknologi internet dalam proses bisnis melalui e-commerce. Aktivitas jual beli pada e-commerce memungkinkan konsumen dan pelaku usaha untuk menyamarkan identitasnya, tanpa dibatasi oleh batas wilayah, dan bahkan lintas Negara. Hal tersebut memungkinkan terjadinya ancaman cybercrime yang merupakan hal serius yang dapat mengganggu aktivitas e- commerce. Penjual dan pembeli harus dapat melindungi diri dari ancaman tersebut melalui cybersecurity. Dalam penelitian ini peneliti berupaya untuk menekankan mengenai pentingnya penerapan cybersecurity sebagai upaya terciptanya keamanan transaksi e-commerce di Indonesia. Pemerintah membuat Undang-Undang sebagai landasan hukum untuk dijadikan acuan apabila terjadi penyalahgunaan dalam pemanfaatan fasilitas yang ada di internet termasuk transaksi elektronik demi menjaga konsumen agar tetap aman dalam bertransaksi.

Kata Kunci: e-commerce, cybercrime, cyberattack, cybersecurity

ABSTRACT

Information technology continues to innovate and transform to become increasingly sophisticated. With the sophistication of this technology, it can provide many conveniences for people's lives, such as integrating internet technology in commercial processes through e-commerce. Buying and selling activities in e-commerce allow consumers and business actors to disguise their identities, without being limited by

Vol.1 No.2
Juni 2023
Hal : 34 – 41

regional boundaries, and even across countries. This allows the occurrence of cybercrime threats which are serious things that can disrupt e-commerce activities. Sellers and buyers must be able to protect themselves from these threats through cybersecurity. In this study, researchers seek to emphasize the importance of implementing cybersecurity as an effort to create secure e-commerce transactions in Indonesia. The government makes laws as a legal basis to be used as a reference if there is abuse in the use of existing facilities on the internet including electronic transactions in order to keep consumers safe in transactions.
Keywords: *e-commerce, cybercrime, cyberattack, cybersecurity.*

A. Latar Belakang

Teknologi informasi bukanlah suatu hal yang sulit untuk didapatkan saat ini, karena sudah masuk ke seluruh lini kehidupan masyarakat. Banyaknya penguna Internet di Indonesia menjadi penanda bahwa internet telah menjadi sebuah kebutuhan bagi masyarakat Indonesia. Teknologi informasi terus berinovasi dan bertransformasi menjadi semakin canggih. Dengan kecanggihannya, teknologi ini bisa memberikan banyak kemudahan bagi kehidupan masyarakat. Salah satu yang dilakukan pelaku usaha yaitu dengan menggunakan teknologi internet dalam proses bisnis sehingga membuat peralihan dari antar muka ke internet. Kita mengenal teknologi ini dengan istilah electronic commerce (e-commerce) atau perdagangan elektronik. Konsep perdagangan secara online yang diusung e-commerce adalah suatu konsep yang memungkinkan penjual dan pembeli tidak perlu bertatap muka secara langsung. Hal ini merupakan salah satu dampak positif dari perkembangan teknologi yang dimanfaatkan dengan baik oleh para pelaku bisnis. Keberadaan e-commerce saat ini tidak hanya menjadi kebutuhan bagi pebisnis, namun telah menjadi kebutuhan bagi para pencari kemudahan berbelanja. Konsumen pekerja yang sibuk adalah pasar paling menjanjikan karena keterbatasan waktu yang dimiliki sedangkan kebutuhan akan suatu barang terus berjalan menjadikan belanja online menjadi alternative terbaik. Munculnya ekonomi digital sebagai model ekonomi yang dominan telah membuat pertukaran moneter lebih mudah diakses oleh orang-orang dari semua latar belakang. Di antaranya adalah tersedianya perangkat lunak pasar yang memanfaatkan web global untuk menyederhanakan langkah-langkah dalam melakukan pembelian atau menawarkan produk (Dewantara et al., 2021).

Era disrupsi ini memaksa pelaku usaha untuk selalu melakukan inovasi agar dapat beradaptasi terhadap kegiatan perdagangan pelaku e-commerce agar memberikan kelancaran dalam proses bisnis sehingga dapat bersaing secara kompetitif. Banyak bentuk layanan yang bisa didapatkan dengan memanfaatkan transaksi e-commerce, mulai dari pembelian tiket transportasi, pembayaran tagihan seperti listrik dan air, kemudian juga layanan perbankan dan investasi. Kehadiran e-commerce sebagai aktivitas jual beli barang atau jasa melalui internet memungkinkan terjadinya cybercrime. Banyak pengguna e-commerce di Indonesia yang memanfaatkannya sebagai aktivitas pembelian atau penjualan produk melalui internet, karena pengguna dapat berkomunikasi dengan menyamarkan identitasnya tanpa dibatasi oleh batas wilayah, dan bahkan lintas negara, sehingga hal tersebut dapat memungkinkan dapat terjadinya ancaman cybercrime. Ancaman terjadinya cybercrime merupakan hal serius yang dapat mengganggu aktivitas e- commerce.

Cybercrime biasanya ditujukan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu operasional proses bisnis. Korban pada cybercrime biasanya terjadi pada pengguna atau pelaku e-commerce itu sendiri yaitu pembeli dan penjual. Konsumen maupun pelaku usaha harus dapat melindungi dirinya dari ancaman tersebut melalui cybersecurity. Cybersecurity atau keamanan siber merupakan tindakan untuk melindungi sistem komputer dari serangan digital atau akses ilegal. Kasus cybercrime di Indonesia dijabarkan dalam temuan Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri yang menangani 4.656 kasus tindak pidana siber sepanjang periode Januari hingga November 2020. Laporan mengenai kasus penipuan online mendominasi di nomor dua dengan 1.295 laporan. Hal ini dapat dijadikan catatan penting terkait tingkat kesadaran akan cybersecurity di Indonesia. Dalam penelitian ini peneliti berupaya untuk menekankan mengenai Pentingnya Penerapan Cyber Security sebagai Upaya Terciptanya Keamanan Transaksi e-Commerce di Indonesia.

B. Metode

Kegiatan pengabdian masyarakat ini dilakukan di Prodi S2 Informatika UIN Sunan Kalijaga Yogyakarta dengan mahasiswa sebagai partisipan. Adapun tahapannya; perencanaan dan pembekalan tim pelaksanan mengenai maksud dan tujuan dengan berkoordianasi dengan ketua Program studi S2 Informatika FST . Pelaksanaan kegiatan; tempat di zoom meeting pada tanggal 30 Maret 2023 oleh dosen dan satu mahasiswa. Langkah pelaksanaan; perijinan pada ketua Program studi S2 Informatika FST, kemudian kegiatan diawali dengan pemberian materi yang menjelaskan manajemen insiden keamanan *cyber security* pemerintahan indonesia agar terciptanya keamanan transaksi *e-commerce* di indonesia.

C. Hasil Dan Pembahasan

Kegiatan pengabdian masyarakat ini dilakukan di Prodi S2 Informatika UIN Sunan Kalijaga Yogyakarta dengan partisipan sejumlah 30 orang. Peserta aktif dalam kegiatan ini dengan bertanya dan melakukan demonstrasi secara langsung. Adapun penjelasan yang diberikan mengenai E-commerce memberikan banyak manfaat bagi konsumen dan para pelaku bisnis. Dengan pembuatan situs penjualan online para penjual dapat dengan mudah melakukan transaksi dengan pembeli tanpa perlu bertatap muka secara langsung. Keberadaan e-commerce saat ini tidak hanya menjadi kebutuhan bagi pebisnis, namun telah menjadi kebutuhan bagi para pencari kemudahan berbelanja. Diantara kemudahan yang dapat dirasakan ternyata ada hal-hal yang harus diwaspadai karena transaksi tersebut melibatkan kegiatan pembayaran yang seringkali menggunakan fasilitas online. Konsumen harus selalu teliti dan bersikap hati-hati dalam memberikan informasi pribadi ketika melakukan transaksi. Materi ini untuk meningkatkan pengetahuan mahasiswa supaya bisa melakukan pengelolaan sistem keamanan siber internal pemerintah indonesia untuk menjamin berkembangnya keamanan e-commerce di indonesia. Kegiatan pengabdian kepada masyarakat yang dilaksanakan berjalan dengan lancar, antusiasme partisipan baik selama mengikuti semua kegiatan.

Sistem keamanan pada e-commerce mencakup beberapa aspek penting yang dijadikan dasar, yaitu aspek-aspek keamanan, macam-macam ancaman, dan solusi dari kekurangan sistem e-commerce. Semua aspek penting pada keamanan e-commerce sangat berpengaruh terhadap tingkat keamanan pada sistem keamanan e-commerce secara keseluruhan. Dalam transaksi jual beli, tentunya pembayaran merupakan bagian yang tak dapat dipisahkan. Pada sistem pembayaran online bisa dikatakan semua cara mengandung resiko.

Beberapa ancaman keamanan yang sering terjadi pada website e-commerce, antara lain credit card fraud atau carding. Carding adalah aktifitas pembelian barang di Internet menggunakan kartu kredit bajakan. Ada beberapa tahapan yang umumnya dilakukan para carder dalam melakukan aksi kejahatannya, yaitu:

1. Mendapatkan nomor kartu kredit yang bisa dilakukan dengan berbagai cara antara lain: phising, hacking, sniffing, keylogging, worm, dan lain-lain. Berbagi informasi antara carder, mengunjungi situs yang memang spesial menyediakan nomor-nomor kartu kredit buat carding dan lain-lain yang pada intinya adalah untuk memperolah nomor kartu kredit;
2. Mengunjungi situs-situs e-commerce seperti Ebay, Amazon untuk kemudian carder mencoba-coba nomor yang dimilikinya untuk mengetahui apakah kartu tersebut masih valid atau limitnya mencukupi;
3. Melakukan transaksi secara online untuk membeli barang seolah-olah carder adalah pemilik asli dari kartu tersebut;

4. Menentukan alamat tujuan atau pengiriman;
5. Pengambilan barang oleh carder.

Pembayaran menggunakan kartu kredit dilakukan dengan menuliskan 3 digit no yang tertera dibelakang kartu dengan demikian apabila kartu tersebut berpindah kepemilikan transaksi tetap dapat dilakukan. Namun beberapa jenis kartu kredit ternama telah mengembangkan sistem keamanan transaksi elektronik yang disebut dengan Secure Electronics Transactions (SET). Berupa protocol enkripsi untuk memberikan keamanan pada konsumen saat transaksi menggunakan kartu kredit. Pembayaran menggunakan internet banking dianggap lebih terpercaya namun tetap harus diwaspadai adanya situs palsu yang dibuat sedemikian rupa menyerupai situs internet banking dan meminta kita memasukkan username dan password.

Untuk penggunaan digital cash, sebuah cara untuk membayar dengan cara mentransfer nilai uang berbentuk elektronik dari satu rekening (account) ke rekening lainnya. Keamanannya dapat diprediksi dari identitas penerima digital cash tersebut. Penyedia layanan digital cash tentu tidak akan begitu saja memberikan charge back jika ternyata terdapat kesalahan/keliru mengirimkan uang ke penerima karena transaksi tersebut terjadi di luar kewenangan penyedia.

Secara umum permasalahan keamanan pada e-commerce sebenarnya berkaitan dengan security

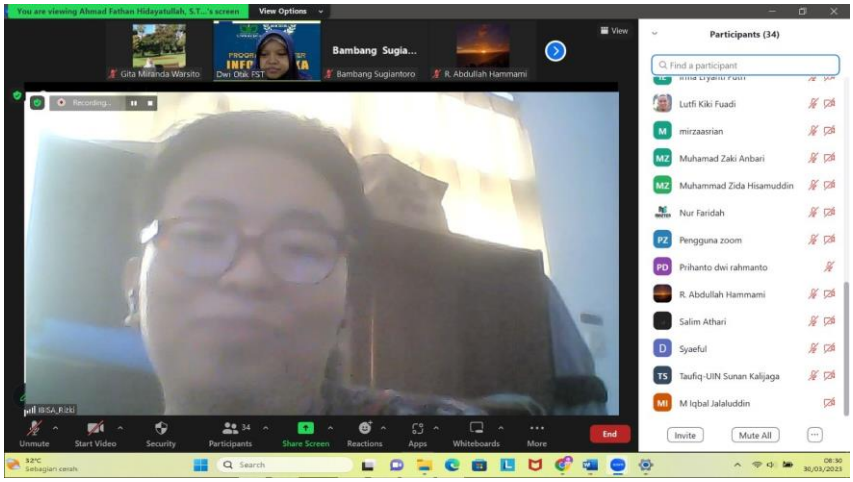
pada web secara umum, diantaranya beberapa aspek yang terkait dengan security web sebagai berikut:

a. Authentication, pemilihan atau penyaringan user dimana hanya user yang legal/terdaftar saja yang dapat bertransaksi menggunakan e-commerce
b. Authorization, yaitu bagaimana melakukan autorisasi, khususnya pada saat proses pembayaran, sehingga data customer dipastikan aman dan terhindar dari hacker
c. Confidentiality atau privacy, yaitu melakukan perlindungan pada data customer dan memastikan keamanannya dari tindak pencurian atau penyadapan oleh hacker untuk digunakan pada transaksi yang semestinya
d. Availability, yaitu terkait dengan ketersediaan sistem dari web server sehingga user dapat senantiasa melakukan transaksi yang aman, kapan saja dan darimana saja.

Data transaksi yang telah diolah oleh sistem dekripsi pada server dapat digunakan oleh sistem e-commerce yang mengadopsinya tanpa melakukan penyesuaian pada sistem web secara keseluruhan. Sistem keamanan pada sistem e-commerce dibuat menggunakan pemrograman berbasis web sehingga sistem keamanan dapat mengamankan data transaksi pada sistem e-commerce tanpa menggunakan protokol keamanan lainnya. Sistem keamanan e-commerce dapat diintegrasikan ke dalam sistem e- commerce sehingga tidak terlihat secara kasat mata oleh pengguna sistem e-commerce tetapi dapat mengamankan data transaksi yang dikirimkan sehingga data transaksi tidak dapat disadap oleh pihak luar dan dapat digunakan pada sistem e-commerce tanpa mengurangi kecepatan loading pada aplikasi maupun web browser.

Dalam pelaksanaannya partisipan diberikan materi yang menitik beratkan pada penjelasan tentang kanker payudara dan bagaimana upaya mendeteksi dini kanker payudara dengan teknik SADARI serta memperagakan bagaimana cara melakukan SADARI. Setelah pemaparan materi partisipan diberikan kesempatan untuk meningkatkan kemapuan melakukan SADARI dengan diminta untuk memperagakan pada phantom dan pada dirinya sendiri.

Gambar 1. Kegiatan penyampaian materi



Gambar 2. Kegiatan Foto Bersama peserta.

Bagi pemilik situs belanja online hendaknya memiliki Standar Operasional Prosedur (SOP) yang cukup jelas tentang prosedur pemesanan dan pengiriman barang. Dengan memastikan keamanan data dan informasi pelanggan untuk melindungi dan meningkatkan reputasi perusahaan serta hubungannya dengan pelanggan, tentunya akan menciptakan kepercayaan pelanggan terhadap perusahaan. Pemilihan teknologi yang efisien dan aman untuk bertransaksi keuangan menjadi tuntutan bagi perusahaan yang bergerak di bidang jasa teknologi keuangan. Demi menjaga konsumen agar tetap aman dalam bertransaksi, Pemerintah membuat Undang-Undang sebagai landasan hukum untuk dijadikan acuan apabila terjadi penyalahgunaan dalam pemanfaatan fasilitas yang ada di internet termasuk transaksi elektronik.

D. Simpulan

Kegiatan pengabdian masyarakat dengan pemberian penyuluhan edukasi manajemen insiden keamanan cyber security pemerintahan indonesia agar terciptanya keamanan transaksi e-commerce di indonesia

E. Saran

Saran kepada Ketua Program studi S2 Informatika FST, untuk melakukan kegiatan serupa secara berkesinambungan untuk meningkatkan kualitas percepatan kelulusan mahasiswa program magister informatika .

F. Ucapan Terimakasih

Selama melakukan pengabdian masyarakat ini peneliti telah banyak mendapat bantuan dari berbagai pihak. Untuk itu dalam kesempatan ini peneliti mengucapkan banyak terimakasih kepada Prodi S1 Sains Data Institut Teknologi Bisnis Dan Kesehatan Bhakti Putra Bangsa Indonesia, Ketua Program studi S2 Informatika FST dan seluruh teman2 mahasiswa S2 Informatika yang telah ikut berpartisipasi dalan pengabdian masyarakat ini.

DAFTAR PUSTAKA

Abdul Halim Barkatullah. 2017. Hukum Transaksi Elektronik di Indonesia. Bandung: Nusamedia.

Aravazhi, M. S. 2020. Understanding Cyber Crime and Cyber Laundering: Threat and Solution. EPRA International Journal of Research and Development (IJRD), 5(1), 34–38. https://doi.org/10.36713/epra2016/.

Cisco. 2021. "What Is a Cyberattack? - Most Common Types. Diakses 27 Desember 2021, dari https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html/.

Dewantara, R., Widiawati, W., Cakranegara, P. A., & Arief, A. S. (2021). Analysis of the Effect of Using Marketplace Based on Customer Data Security. Jurnal Mantik, 6(3), 1–11. https://iocscience.org/ejournal/index.php/mantik/article/view/3018

IBM. 2021. What is a cyber attack? Diakses 27 Desember 2021, dari https://www.ibm.com/id-en/topics/cyber-attack/.

Irfan, M., Ramdhani, M. A., Darmalaksana, W., Wahana, A., & Utomo, R. G. 2018. Analyzes of Cybercrime Expansion in Indonesia and Preventive Actions. IOP Conference Series: Materials Science and Engineering, 434(012257), 1–6. https://doi.org/10.1088/1757-899X/434/1/012257/.

ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity

Nazir, Moh., 2017. Metode Penelitian. Bogor: Ghalia Indonesia.

Rerung, Rintho Rante. 2018. E-Commerce: Menciptakan Daya Saing Melalui Teknologi Informasi. Yogyakarta: Deepublish.

Shekar, B., & Prabha, A. 2020. Impacts of Cyber Crime on the Victims. UGC Care Journal, 40(50), 2731–2737. https://digital.wings.uk.barclays/for-everyone/milestone/impacts-ofcyber-crime/.

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik (UU ITE)

Unisys. 2021. Cyber Attack Definition. Diakses 27 Desember 2021, dari https://www.unisys.com/glossary/cyberattack/.

Vermaat, Misty E., Susan L. Sebok, Steven M. Freund, Jennifer T. Campbell, dan Mark Frydenberg. 2018. Discovering Computers 2018 – Digital Technology, Data and Devices. United States: Cengage.