Pelatihan Penangkalan Peretasan Data Kegiatan UMKM untuk Meningkatkan Pertumbuhan Ekonomi di Kecamatan Medan Perjuangan Kota Medan

Bambang Sugiharto[1], Harkim[2], Edison Parulian[3], Agus Marwan[4]
[1]Universitas Pemabinaan Masyarakat Indonesia, [2,4]STIE Profesional Indonesia, [3]Universitas IBBI, Indonesia
E-mail: iqbalhibat@gmail.com, safaat.yulianto@itesa.ac.id

Article Info
Article History
Received: 2024-06-23
Revised: 2024-07-21
Published: 2024-08-09

Keywords:
Hacking;
MSMEs;
Data;
Growth;
Economy.

Abstract
Data is an elementary thing in various organizational activities, in this context it is data dealing with MSME activities in the Medan Perjuangan sub-district, Medan City. Data becomes an asset which indirectly is capital for determining and planning further programs. In this PKM activity, the method used is a lecture using learning aids or learning media in the form of PPT material and also videos with content relevant to the theme of service. The results of the service are (1) a clearer understanding of company data by the beneficiary community, (2) increased public awareness of securing company data (3) adding software and hardware to make data safer.

Artikel Info
Sejarah Artikel
Diterima: 2024-06-23
Direvisi: 2024-07-21
Dipublikasi: 2024-08-09

Kata kunci:
Peretasan;
UMKM;
Data;
Pertumbuhan;
Ekonomi.

Abstrak
Data menjadi hal yang elementer dalam berbagai aktivitas organisasi, dalam konteks ini adalah data mengani kegitan UMKM di kecamatan Medan Perjuangan Kota Medan. Data menjadi aset yang secara tidak langsung adalah modal untuk penentuan dan perencanaan program lebih jauh. Dalam kegiatan PKM kali ini, metode yang digunakan adalah ceramah yang menggunakan alat bantu belajar atau media pembelajaran berupa PPT materi dan juga video dengan konten relevan dengan tema pengabdian. Hasil pengabdian adalah (1) pemahaman yang lebih jelas tentang data perusahaan oleh masyarakat penerima manfaat, (2) kesadaran masyarakat untuk mengamankan data perusahaan menjadi meningkat (3) melakukan penambahan sofware dan hardware agar data menjadi lebih aman.

I. PENDAHULUAN

Peretasan secara luas didefinisikan sebagai eksploitasi kerentanan dalam sistem dan jaringan komputer organisasi untuk mendapatkan akses atau kendali tidak sah atas aset digital. Aktivitas ini melibatkan identifikasi kelemahan dalam sistem atau jaringan komputer dan eksplorasi lebih lanjut serta manipulasi informasi dengan niat jahat atau motivasi diri. Dalam banyak kasus, peretasan melibatkan kombinasi pengetahuan teknis, keterampilan memecahkan masalah, kreativitas, dan ketekunan – semuanya untuk melewati langkah-langkah keamanan dan mengakses informasi pribadi atau basis data yang dilindungi. Meskipun beberapa bentuk peretasan "topi putih" dapat dilakukan secara etis untuk meningkatkan keamanan, peretasan ini paling sering dilakukan dengan tujuan mencuri data sensitif, menyusupi sistem, atau menyebarkan virus dan malware.

Pasar rakyat selain merupakan wadah aktivitas perdagangan juga merupakan wadah Usaha Mikro, Kecil dan Menengah (UMKM) untuk berkembang dengan diiringi nilai sosial budaya yang khas dari suatu wilayah. Hal ini menjadikan pasar rakyat sebagai pondasi dasar bagi perekonomian wilayah dan perekonomian rakyat. Di sisi lain, dengan muncul dan berkembangnya pasar modern dan pusat perbelanjaan yang dikelola oleh swasta, eksistensi pasar rakyat semakin tergerus (Rahmi & Riyanto, 2022). Data Kementerian Koperasi dan UKM RI (2020) menunjukkan bahwa selama tahun 2020, terdapat sekitar 10,2 juta UMKM yang menggunakan teknologi digital dalam kegiatan usahanya. Angka ini meningkat kurang lebih 13 persen dibandingkan dengan tahun sebelumnya.

Meskipun di satu sisi pemanfaatan teknologi digital memungkinkan pelaku UMKM tetap terhubung dengan konsumen dan dapat menjangkau konsumen baru serta meningkatkan pendapatan, adaptasi digital juga memiliki risiko, diantaranya risiko siber seperti penipuan online, peretasan, pemalsuan identitas, dan bocornya data konsumen. Terlebih kecerdasan buatan telah mendominasi jejaring digital pada berbagai bidang. Bisa saja kecerdasan buatan mencuri berbagai data. Mengenali tentang AI tidaklah sulit, karena sesungguhnya dalam keseharian aktivitas yang kita lakukan, telah bersinggungan dengan penggunaan AI. Dalam perkembangannya teknologi dan informasi sampai saat ini sudah benar-benar cepat dan tanpa di sadari sudah

benar-benar mempengaruhi aspek dalam kehidupan manusia (Kalsum, 2022). Edukasi mengenai keamanan siber sebagai upaya untuk meningkatkan kesadaran dan budaya keamanan siber menjadi salah satu upaya penting yang dapat dilakukan oleh berbagai pihak seperti perusahaan, asosiasi, dan pemerintah secara sinergis dalam rangka mencegah kerugian yang lebih besar lagi. Parahnya lagi, mayoritas perusahaan dinilai tidak memiliki rencana mitigasi terhadap serangan siber.

Mayoritas serangan siber yang terjadi ditujukan pada usaha kecil, dan kesalahan manusia merupakan salah faktor terbesar yang mempengaruhi keamanan siber sebuah perusahaan. Kurangnya pemahaman akan keamanan siber juga dianggap sebagai penyebab utama mengapa masih banyak pelaku usaha, termasuk UMKM, sangat rentan terhadap kejahatan di jagat maya. Salah satu tantangan digitalisasi UMKM di Indonesia adalah rendahnya tingkat literasi digital. Rendahnya literasi menjadi faktor penting yang menyebabkan rentannya UMKM terhadap serangan siber. Kami menyambut baik kegiatan literasi tentang keamanan informasi secara rutin dilakukan oleh industri fintech. Diharapkan, para pelaku usaha UMKM ke depannya dapat lebih siap dalam menerapkan prinsip-prinsip keamanan informasi.

II. METODE PENELITIAN

Dalam kegiatan PKM kali ini, metode yang digunakan adalah ceramah yang menggunakan alat bantu belajar atau media pembelajaran berupa PPT materi dan juga video dengan konten relevan dengan tema pengabdian. Dari metode ceramah diharapkan kognisi dan afeksi peserta sosialisasi akan mendapatkan pengetahuan dan akhirnya menentukan sikap betapa pentingnya kesaadaran akan perlindungan data kegiatan UMKM di wilayah mereka. Metode lanjutnya adalah learning by doing dengan mencoba mempraktekkan bagaimana memberikan proteksi digital atas data – data tersebut, dengan menggunakan laptop yang sebelumnya telah dipersiapkan oleh peserta sosialisasi.

III. HASIL DAN PEMBAHASAN

Pentingnya para pelaku UMKM dengan dunia teknologi akan membantu memudahkan hidupnya. Tanpa memiliki kemampuan untuk menalar dengan baik, manusia dengan segudang pengalaman dan pengetahuan tidak akan dapat menyelesaikan masalah dengan baik. Demikian juga dengan kemampuan menalar yang sangat baik, namun tanpa bekal pengetahuan dan pengalaman yang memadai, manusia juga tidak akan bisa menyelesaikan masalah dengan baik(Sobron & Lubis, 2021). Technopreneurship gabungan dari kata technology dan entrepreneur (Sanny et. al, 2016). Saat ini, peretasan komputer dan jaringan hadir dalam berbagai bentuk, mulai dari serangan injeksi SQL yang rumit hingga serangan penolakan layanan yang lebih tradisional. Walaupun sebagian besar teknik peretasan tersebut tumpang tindih dengan bentuk umum serangan siber, beberapa jenis peretasan siber yang paling umum meliputi:

Serangan Perangkat Lunak Jahat. Perangkat lunak berbahaya, juga dikenal sebagai malware , yang menginfeksi sistem dan menyebar tanpa sepengetahuan atau persetujuan pengguna, merusak file, mencuri data, atau mendapatkan akses tidak sah. Dalam era digital, kejahatan siber (cybercrime) tidak hanya berpotensi merusak data dan informasi pribadi, tetapi juga dapat menghancurkan aktivitas ekonomi dan bisnis, infrastruktur, dan bahkan stabilitas keamanan nasional suatu negara. Cybercrime merupakan kejahatan yang dilakukan dengan memanfaatkan teknologi informasi dan komunikasi (TIK), sedangkan cybersecurity ditujukan sebagai upaya untuk melindungi sistem komputer dari berbagai ancaman atau akses ilegal.

Cyberattack atau serangan siber adalah serangan yang dilakukan oleh pelaku kejahatan siber dengan menggunakan satu atau lebih komputer terhadap satu atau beberapa komputer atau jaringan. Hal ini menjadi perhatian serius bagi individu, perusahaan, dan pemerintah. Indonesia tidak terlepas dari berbagai serangan siber. Data statistik dari Badan Siber dan Sandi Negara (BSSN) mencatat bahwa telah terjadi 370,02 juta serangan siber terhadap Indonesia pada tahun 2022. Dibandigkan dengan tahun sebelumnya (terjadi 266,74 juta serangan siber), jumlah ini meningkat sebesar 38,72%. Sektor administrasi pemerintahan menjadi target utama serangan siber di Indonesia dengan serangan berjumlah 284,09 juta. Pemerintah Indonesia juga telah mengeluarkan peraturan untuk melindungi sistem komputer dari serangan digital atau akses ilegal, seperti Undang-Undang Informasi Transaksi Elektronik (UU ITE). UU ITE tak hanya menjadi pelindung masyarakat di dunia digital namun menjadi aturan bersama bagi masyarakat yang beraktifitas di dunia digital.

Serangan Ransomware. Ransomware adalah bentuk malware tingkat lanjut yang meng-enkripsi data korban dan meminta pembayaran tebusan agar dapat melepaskan dan memulihkan

akses ke file atau sistem secara efektif. Ransomware pertama kali muncul pada awal tahun 1990-an dan dikenal sebagai "AIDS Trojan" atau "PC Cyborg". Ransomware awal ini mengunci akses ke sistem dengan mengenkripsi file dan meminta tebusan dalam bentuk cek yang harus dikirim ke kotak surat tertentu. Namun, ransomware modern yang menggunakan kriptocurrency sebagai metode pembayaran pertama kali muncul pada tahun 2005 dengan munculnya varian ransomware bernama "GpCode". Sejak itu, serangan ransomware telah terus berkembang dan menjadi ancaman serius di dunia digital. Adapun secara umum jenis-jenis ransomware dapat dibedakan menjadi berikut:

Encrypting Ransomware, Jenis ini merupakan bentuk yang paling umum dari ransomware. Ransomware ini menggunakan algoritma enkripsi yang kuat untuk mengenkripsi file pengguna sehingga tidak dapat diakses tanpa kunci dekripsi yang benar. Contoh terkenal dari encrypting ransomware adalah WannaCry dan CryptoLocker. Locker Ransomware, Berbeda dengan encrypting ransomware, locker ransomware tidak mengenkripsi file, tetapi memblokir akses ke sistem secara keseluruhan. Biasanya, locker ransomware akan menampilkan pesan yang menghalangi pengguna untuk mengakses komputer mereka. Ransomware jenis ini sering kali menyamar sebagai pemberitahuan palsu dari pihak berwenang, seperti kepolisian atau badan keamanan.

MBR Ransomware, Ransomware yang menyerang Master Boot Record (MBR) komputer atau perangkat. MBR berperan dalam proses booting sistem operasi, dan ransomware jenis ini akan menggantikan MBR dengan kode yang memblokir akses ke sistem. Hal ini menyebabkan perangkat menjadi tidak dapat digunakan hingga tebusan dibayar atau MBR dikembalikan. Mobile Ransomware, Ransomware yang dirancang khusus untuk menyerang perangkat mobile, seperti smartphone atau tablet. Mobile ransomware dapat mengenkripsi data pada perangkat atau memblokir akses ke aplikasi dan fungsi penting. Salah satu contohnya adalah Android/ Filecoder. C, yang menargetkan perangkat Android.

Scareware, Ransomware yang menggunakan taktik penipuan dengan menampilkan pesan ancaman palsu kepada pengguna. Pesan ini berisi peringatan palsu tentang pelanggaran hukum atau kegiatan ilegal yang diduga dilakukan oleh pengguna. Tujuannya adalah untuk menakut-nakuti pengguna agar membayar tebusan.

Serangan Phishing. Phishing adalah upaya penipuan untuk menangkap informasi sensitif (seperti kata sandi, kredensial login, atau data keuangan) dengan berpura-pura menjadi entitas yang sah atau dapat dipercaya melalui email, telepon, atau situs web. Phising adalah kejahatan digital yang menargetkan informasi atau data sensitif korban melalui email, unggahan media sosial, atau pesan teks. Istilah phising adalah bentuk lain dari kata phishing yang berasal dari bahasa Inggris ‘fishing’ yaitu memancing. Bisa dibilang, aktivitas phising adalah bertujuan memancing orang untuk memberikan informasi pribadi secara sukarela tanpa disadari untuk tujuan kejahatan. Dengan kata lain, arti phising adalah serangan yang dilakukan untuk menipu atau memancing korban agar mau mengklik link atau tautan serta menginput informasi kredential seperti username dan password. Pelaku phising adalah biasanya menampakkan diri sebagai pihak atau institusi yang berwenang. Mereka menyisipkan tautan di dalam narasi yang disebarkan, dan menggiring korban agar mengeklik tautan tersebut.

Serangan Brute Force. Serangan brute force adalah metode coba-coba yang digunakan pelaku ancaman untuk memecahkan kata sandi atau kunci enkripsi dengan mencoba secara sistematis setiap kemungkinan kombinasi hingga kombinasi yang benar ditemukan. Ini bisa memakan waktu tetapi sering kali efektif terhadap kata sandi yang lemah atau sederhana. Serangan brute force adalah metode peretasan yang menggunakan uji coba untuk memecahkan kata sandi, kredensial login , dan kunci enkripsi. Ini adalah taktik sederhana namun andal untuk mendapatkan akses tidak sah ke akun individu dan sistem serta jaringan organisasi. Peretas mencoba beberapa nama pengguna dan kata sandi, sering kali menggunakan komputer untuk menguji berbagai kombinasi, hingga mereka menemukan informasi login yang benar.

Nama "brute force" berasal dari penyerang yang menggunakan upaya yang sangat kuat untuk mendapatkan akses ke akun pengguna. Meskipun merupakan metode serangan siber lama, serangan brute force telah dicoba dan diuji serta tetap menjadi taktik yang populer di kalangan peretas. Kecerdasan buatan adalah proses analisis berbasis komputer yang cenderung menciptakan sistem komputasi yang kita akan cenderung untuk disebut cerdas (Mulyatun et al., 2021).

Gambar 1. Pelaksanaan PKM

Gambar 2. Peserta Mendengarkan Paparan NaraSumber

Tahap implementasi merupakan tahap lanjut dari kegiatan perancangan. Tujuan pada tahap ini adalah untuk mengetahui apakah sistem ini dapat dapat berjalan dengan baik sesuai dengan perancangan sistem yang telah dibuat sebelumnya (Mashud & Wisda, 2019). Maka dalam pengabdian ini para peserta akan menerapkan bagaimana keamanan sistem data yang ada pada platform digital UKM nya. Saat ini ancaman keamanan siber kian meningkat dua kali lipat. Sebelumnya, tren ancaman ini berada di angka 200 juta. Hingga akhir tahun 2020, tren ini naik hingga lebih dari 495 ancaman kemanan siber. UMKM merupakan salah satu sektor yang juga diserang. Menurut Data Breach Investigations Report, 43 persen dari serangan siber menarget UMKM, dan hanya 14 persen UMKM yang sudah mempersiapkan diri menghadapi ancaman tersebut. Kini para pelaku UMKM di wilayah ini sudah menyadari pentingnya keamanan siber bagi data yang dimilikinya, sehingga ancaman peretasan dapat ditanggulangin dengan baik.

IV. SIMPULAN DAN SARAN

A. Simpulan

Data memang kebutuhan yang sifatnya elementer dalam sebuah konstruksi bisnis yang sedang berjalan. Keamanannya perlu ditingkatkan agar pratik pencurian data data di proteksi semaksima mungkin. UMKM memiliki peran yang cukup signifikan dalam meningkatkan kesejahteraan masyarakat. Dimulai dari pendapatan, dengan adanya UMKM pastinya akan menyerap tenaga kerja lebih banyak sehingga pendapatan masyarakat juga semakin tinggi. Selain itu, pendapatan yang tinggi dapat memenuhi kebutuhan rumah tangga masyarakat seperti halnya meningkatnya daya beli masyarakat(Aliyah, 2022). Hasil pengabdian adalah (1) pemahaman yang lebih jelas tentang data perusahaan oleh masyarakat penerima manfaat, (2) kesadaran masyarakat untuk mengamankan data perusahaan menjadi meningkat (3) melakukan penambahan sofware dan hardware agar data menjadi lebih aman.

B. Saran

Pembahasan terkait penelitian ini masih sangat terbatas dan membutuhkan banyak masukan, saran untuk penulis selanjutnya adalah mengkaji lebih d alam dan secara komprehensif tentang Pelatihan Penangkalan Peretasan Data Kegiatan UMKM untuk Meningkatkan Pertumbuhan Ekonomi.

DAFTAR RUJUKAN

Aliyah, A. H. (2022). Peran Usaha Mikro Kecil dan Menengah (UMKM) untuk Meningkatkan Kesejahteraan Masyarakat. *WELFARE Jurnal Ilmu Ekonomi*, *3*(1), 64–72. https://doi.org/10.37058/wlfr.v3i1.4719

Kalsum, U. (2022). Pengenalan Kecerdasan Buatan (Artificial Intelligence) Kepada Para Remaja. *Procedia Computer Science*, *166*, 310–314. https://www.binadarma.ac.id

Mashud, M., & Wisda, W. (2019). Aplikasi Chatbot Berbasis Website sebagai Virtual Personal Assistant dalam Pemasaran Properti. *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi*, *9*(2), 99. https://doi.org/10.35585/inspir.v9i2.2497

Mulyatun, S., Utama, H., & Mustopa, A. (2021). PENDEKATAN NATURAL LANGUAGE PROCESSING PADA APLIKASI Sistem Informasi Universitas Amikom Yogyakarta Abstraksi Keywords : Pendahuluan. *Jurnal of Information System Management*, *2*(1), 12–17.

Rahmi, J., & Riyanto, R. (2022). Dampak Upah Minimum Terhadap Produktivitas Tenaga Kerja: Studi Kasus Industri Manufaktur

Indonesia. *Jurnal Ekonomi Dan Kebijakan Publik*, *13*(1), 1–12. https://doi.org/10.22212/jekp.v13i1.2095

Sanny et. al, E. (2016). *Konsep Dasar Technopreneurship*.

Sobron, M., & Lubis. (2021). Implementasi Artificial Intelligence Pada System Manufaktur Terpadu. *Seminar Nasional Teknik (SEMNASTEK) UISU*, *4*(1), 1–7. https://jurnal.uisu.ac.id/index.php/semnastek/article/view/4134