

Security Awareness Framework untuk Usaha Mikro, Kecil dan Menengah di Indonesia

Abdul Azzam Ajhari¹⁾, Mawidyanto Agustian Manaon²⁾, Dimas Febriyan Priambodo³⁾

(1) Deputy Bidang Keamanan Siber dan Sandi Perekonomian, Badan Siber dan Sandi Negara, abdul.azzam@bssn.go.id

(2) Deputy Bidang Keamanan Siber dan Sandi Perekonomian, Badan Siber dan Sandi Negara, mawidyanto.agustian@bssn.go.id

(3) Rekayasa Keamanan Siber, Politeknik Siber dan Sandi Negara, dimas.febriyan@poltekssn.ac.id

Abstrak

Perkembangan teknologi yang semakin masif memiliki dampak positif dan negatif terhadap kegiatan bisnis. Dampak ini terjadi akibat berbagai tindakan kejahatan dunia maya yang mengikuti perkembangan teknologi yang digunakan. Serangan siber terhadap pelaku atau pemilik usaha mikro, kecil, dan menengah (UMKM) dapat mengakibatkan risiko kerugian reputasi dan keuangan. Langkah-langkah perlindungan diperlukan untuk mencegah kerugian tersebut, dimulai dengan meningkatkan pemahaman mengenai pentingnya keamanan informasi. Penelitian ini bertujuan untuk mengkaji metodologi dan hasil Pedoman Penilaian Keamanan Informasi (PAMAN KAMI) yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN). National Institute of Standards and Technology Interagency Report 7621 Revision 1 (NISTIR 7621 Rev 1) adalah kerangka kerja keamanan siber untuk mengukur usaha kecil, namun perlu disesuaikan agar mudah dipahami dan digunakan. PAMAN KAMI mengubahnya menjadi pertanyaan yang dapat dijawab sendiri. Kesadaran dan kematangan keamanan siber diukur pada tahun 2020 - 2022 dengan total 964 UMKM berpartisipasi. Namun, hanya 844 UMKM yang mengisi PAMAN KAMI dengan hasil penilaian didominasi oleh kategori BURUK dan KURANG. Penelitian ini juga memvalidasi tingkat literasi keamanan informasi, terutama di UMKM, sehingga dapat digunakan sebagai dasar untuk langkah-langkah mitigasi siber.

Kata kunci: BSSN, Keamanan Informasi, Maturity Test, Self Assessment, UMKM.

Abstract

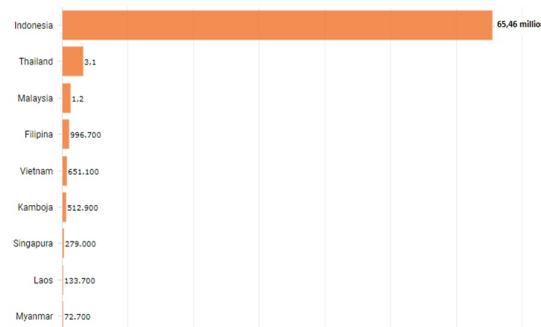
Technological developments that are increasingly massive have positive and negative impacts on business activities. This impact occurs from various cybercrimes following the development of the technology used. Cyberattacks on perpetrators or owners of micro, small, and medium enterprises (MSMEs) can result in the risk of reputational and financial loss. Protection measures are needed to prevent such losses, starting with increasing understanding regarding the importance of information security. This study attempts to examine the methodology and results of the information security self-assessment guidelines (PAMAN KAMI) issued by the National Cyber and Crypto Agency (BSSN). National Institute of Standards and Technology Interagency Report 7621 Revision 1 (NISTIR 7621 Rev 1) is a cybersecurity framework for measuring small businesses, but it needs customization to be easy to understand and use. PAMAN KAMI turned it into self-assessable questions. Cybersecurity awareness and maturity were measured in 2020 – 2022 with a total of 964 MSMEs participating. However, only 844 MSMEs filled out PAMAN KAMI with assessment results dominated by the BAD and LESS categories. This study also validates the level of information security literacy, especially in MSMEs, so that it can be used as a basis for cyber mitigation measures.

Keywords: BSSN, Information Security, Maturity Test, MSMEs, Self Assessment.

1. PENDAHULUAN

Indonesia memiliki jumlah usaha mikro, kecil, dan menengah (UMKM) tertinggi di kawasan ASEAN berdasarkan data Laporan Investasi ASEAN yang dirilis pada September 2022 [1], terlihat dalam Gambar 1. Kontribusi UMKM pada tahun 2022 mencapai 60,5% [2] PDB atau Rp 11.850,9 triliun dimana perkiraan PDB nasional secara keseluruhan mencapai Rp 19.588,4 triliun [3]. UMKM juga berperan dalam penyerapan lapangan kerja yang mencapai 96,9% dari total penyerapan lapangan kerja nasional [4].

Pada tahun 2021, setidaknya terdapat 65,46 juta UMKM di Indonesia yang ditunjukkan pada Gambar 1. Tingginya jumlah UMKM di Indonesia memerlukan perhatian serius dari pemerintah dalam mengelola pertumbuhan ekonomi secara digital.



Gambar 1. ASEAN Investment Report 2022

Kurangnya kesadaran para pelaku usaha dalam mengelola dan mengamankan datanya membuat mereka rentan terhadap risiko kejahatan siber [5]. Faktor sumber daya manusia (SDM) berpengaruh terhadap pertumbuhan UMKM, dan secara parsial

faktor keamanan siber berpengaruh terhadap pertumbuhan UMKM [6].

Salah satu kegiatan yang dapat dilakukan adalah mendukung para pelaku UMKM dalam meningkatkan pemahamannya terhadap kesadaran keamanan siber. Biasanya pelatihan dilakukan dengan memberikan pembekalan secara personal kepada Usaha Kecil Menengah (UKM) agar sumber daya manusia dapat meningkatkan prestasi kerja dan menambah pengetahuan tentang apa saja yang dibutuhkan UKM untuk berinovasi dan mencapai tujuan [7].

Literasi digital telah dilakukan dalam penelitian [8] dengan memberikan pemahaman tentang risiko kejahatan dunia maya yang umum seperti *phishing*, *spamming*, *malware*, dan *ransomware*. Kemudian, pendidikan kesadaran keamanan siber telah dilakukan dalam penelitian [9] dengan memulai dari tahap analisis situasi untuk mengidentifikasi permasalahan risiko dan pemahaman terkait keamanan siber pada pelaku usaha.

Selain itu menurut hasil penelitian [10] bahwa bisnis yang dikelola secara tim memiliki kerentanan yang lebih tinggi dibandingkan bisnis yang dikelola secara individu. Beberapa permasalahan kerentanan yang sering menjadi permasalahan adalah kekuatan *password*, akses internet dan *file sharing* yang kurang aman, serta banyaknya serangan *phishing* pada email [11].

Meningkatnya pemahaman terhadap kesadaran keamanan siber dapat mendorong pelaku UMKM untuk mampu melakukan Penilaian Mandiri Keamanan Informasi (PAMAN KAMI) yang menjadi pedoman Badan Siber dan Sandi Negara (BSSN) untuk menilai kematangan keamanan siber UMKM. Sehingga hasil penilaian tersebut dapat meningkatkan kesadaran pengelolaan keamanan informasi mulai dari pelaku usaha itu sendiri. PAMAN KAMI telah melalui beberapa tahapan pengembangan sejak awal tahun 2019 untuk versi 1 yang dikembangkan pada tanggal 20 September 2019 (versi 1.1) dengan uji coba agar lebih *user-friendly* dan mengakomodasi Statement of Applicability (SoA) [12] dan validasi oleh pelaku usaha bersama Auditor Keamanan Informasi Baderi dan Eko Tulus Budi Cahyanto di Kota Balikpapan. Perubahan PAMAN KAMI selanjutnya dilakukan di Jakarta berdasarkan hasil pengujian dan validasi instrumen bagi pelaku usaha di Kota Semarang (versi 1.2), *start-up* di Kota Makassar (versi 1.3), dan *start-up* di Kota Batam (versi 2.0).

Riset [13] telah menggunakan PAMAN KAMI untuk melakukan survei terhadap 103 pelaku UMKM dengan menunjukkan bahwa 50,48% dari total UMKM yang disurvei telah mencapai indikator kategori CUKUP. Diperlukan penelitian lebih lanjut dengan lebih banyak data untuk lebih memvalidasi hasil penilaian UMKM di Indonesia secara keseluruhan. Sebagai enam aturan praktis untuk menentukan ukuran sampel dan kekuatan statistik [14], aturan pertama adalah sampel yang lebih besar

meningkatkan kekuatan statistik evaluasi. Aturan kedua adalah mengevaluasi kebutuhan sampel yang lebih besar untuk mencapai tingkat kekuatan tertentu. Aturan ketiga adalah mengevaluasi program dengan penyerapan rendah yang memerlukan sampel lebih besar. Aturan keempat adalah jika populasi yang mendasari mempunyai variasi hasil yang tinggi, evaluasi memerlukan sampel yang lebih luas. Aturan kelima adalah memaksimalkan kekuatan untuk ukuran sampel tertentu ketika sampel dibagi rata antara kelompok perlakuan dan kelompok kontrol. Aturan terakhir adalah pengacakan pada tingkat kelompok dibandingkan pada tingkat individu akan mengurangi kekuatan evaluasi untuk sampel tertentu. Semakin mirip hasil individu-individu dalam klaster, semakin besar sampel yang dibutuhkan.

Pada tahun 2020-2022, BSSN melalui Direktorat Keamanan Siber dan Kriptografi Keuangan, Perdagangan, dan Pariwisata melakukan pengukuran kematangan keamanan siber pada UMKM menggunakan PAMAN KAMI yang dilakukan di wilayah Solo, Ambon, Banjarmasin, Likupang, Kupang, Bali, Labuan Bajo, Lombok, dan Bangka. Lokasi tersebut dipilih karena memiliki Dinas Koperasi, UKM yang mewadahi dan memfasilitasi penumbuhan dan peningkatan kualitas daya saing pelaku UMKM. Kegiatan ini bertujuan untuk mengukur tingkat kematangan keamanan siber di sektor UKM wilayah tersebut menggunakan PAMAN KAMI.

2. LANDASAN TEORI

Pedoman PAMAN KAMI memiliki 5 (lima) instrumen yaitu identifikasi, perlindungan, deteksi, respon, dan pemulihan. Setiap *item* pertanyaan penilaian disesuaikan dan diadopsi dengan kerangka keamanan siber dalam National Institute of Standards and Technology Interagency Report 7621 Revisi 1 (NISTIR 7621 Rev 1) tentang *Small Business Information Security: The Fundamentals* [15].

Untuk instrumen identifikasinya dipetakan ke dalam pertanyaan-pertanyaan berupa identifikasi aset kritis, identifikasi risiko, serta pembuatan prosedur dan kebijakan keamanan informasi. Sedangkan instrumen proteksi berisi pertanyaan untuk menilai penggunaan seluruh *password* pada semua perangkat, pengelolaan *password*, perlindungan terhadap kehilangan atau kebocoran informasi penting perusahaan, perawatan area penting perusahaan, proteksi lonjakan arus, dan memastikan informasi penting yang telah terbuang tidak dapat digunakan kembali. Instrumen perlindungan berisi pertanyaan untuk menilai kehati-hatian dalam menggunakan *wifi* publik, rekayasa sosial, dan melakukan pembaruan keamanan perangkat secara otomatis. Proteksi juga digunakan untuk mengukur instalasi aplikasi dari sumber tidak dikenal, kebijakan penggunaan internet perusahaan, dan program edukasi keamanan informasi untuk akses karyawan pada jam kerja,

penggunaan *firewall*, dan *password* yang kuat pada penggunaan wifi perusahaan.

Instrumen pendeteksi berisi pertanyaan yang berfokus pada pelaksanaan instalasi antivirus secara berkala dan pembaruan basis data, langkah-langkah untuk memastikan keamanan *e-mail* yang diterima, dan mencatat setiap akses sistem. Instrumen respons berisi pertanyaan mengenai rencana tindak lanjut atas kebocoran, kehilangan, atau pencurian aset penting perusahaan. Terakhir, instrumen pemulihan berisi pertanyaan untuk mengukur pencadangan rutin dan pembelajaran serta literasi tentang metode serangan siber terkini dan ancaman terhadap internal perusahaan.

3. METODE PENELITIAN

PAMAN KAMI v2.0 merupakan metode yang berfokus pada 25 langkah pengamanan informasi bagi UMKM [13] dan digunakan dalam penelitian ini. Selain itu, instrumen PAMAN KAMI memiliki kesamaan metode [16] terkait dengan pendekatan keamanan lapisan manusia, keamanan lapisan perimeter fisik & logis, keamanan lapisan jaringan, keamanan lapisan *host/endpoint*, keamanan lapisan aplikasi, keamanan lapisan data, dan aset-aset penting. Langkah-langkah tersebut terbagi menjadi dua bagian, yaitu penilaian mandiri (PAMAN) dan keamanan informasi (KAMI).

3.1 Penilaian Mandiri

Penilaian diri merupakan suatu proses dimana seseorang mengevaluasi dan memeriksa dirinya sendiri untuk mengetahui kelebihan dan kekurangannya, serta untuk meningkatkan kinerja dan kemampuannya. Pengusaha dapat melakukan penilaian mandiri terhadap keamanan siber dan penggunaan teknologi informasi yang ada.

Pengguna akan diminta menjawab serangkaian pertanyaan terkait keamanan siber dan penggunaan teknologi informasi. Pertanyaan-pertanyaan tersebut mencakup berbagai aspek, seperti penggunaan kata sandi yang kuat, pembaruan sistem dan anti-virus secara berkala, serta tindakan pencegahan terhadap serangan siber dengan daftar tabel 1 berikut ini.

Tabel 1. Pertanyaan Penilaian Diri

No	Question	Assessment Point			
		DM	DS	TD	TT
1	Have you identified important business (company) assets that must be protected?	4	2	0	0
2	Have you identified all possible risks of losing important business (company) assets?	4	2	0	0
3	Do you have procedures and information security policies in place to protect important business (company) assets?	4	2	0	0

No	Question	Assessment Point			
		DM	DS	TD	TT
4	Do you implement the use of <i>passwords</i> on computers, laptops, and/or smartphones to prevent data theft?	4	2	0	0
5	Have you created a <i>password</i> that is strong and not easy to guess and do not use the same <i>password</i> for multiple Accounts (web services)?	4	2	0	0
6	Do you implement steps to prevent loss or leakage of important information, such as keeping important information in locked cabinets/cupboards/drawers, and not leaving it on the table?	4	2	0	0
7	When you see someone you don't know entering the restricted work area belonging to the business (company), do you protect yourself by approaching and asking for the purpose and purpose of the person's arrival?	4	2	0	0
8	Have you installed electronic surge protectors and Uninterruptible Power Supplies (UPS) to protect business network devices from lightning strikes, power surges, or short circuits?	4	2	0	0
9	When removing/deleting important information, have you made sure that the important information that was removed/deleted becomes unreadable, such as using a paper shredder/data deletion tool?	4	2	0	0
10	Do you apply a policy of not connecting your computer, laptop, and smartphone with a public internet network (Wi-Fi) when accessing important accounts?	4	2	0	0
11	Do you adopt ways to avoid social engineering attacks such as limiting the private information that is shared publicly or being skeptical of strangers wanting to know your sensitive information?	4	2	0	0
12	Do you always keep your Operating System, smartphone, software and business applications (company) getting security updates from vendors/providers automatically?	4	2	0	0
13	Do you always ensure that the applications you download and install on your business (company) computers, laptops, and	4	2	0	0

No	Question	Assessment Point			
		DM	DS	TD	TT
	smartphones are safe and come from trusted sources?				
14	Do you have policies in place to control Internet use, such as setting rules about browsing websites and posting to social media on work area (office) computers?	4	2	0	0
15	Do you have a program to educate employees about the importance of information security and that information security is the responsibility of everyone who works for your business (company)?	4	2	0	0
16	Do you require business partners to maintain confidentiality, such as including nondisclosure clauses (obligation to maintain confidentiality) in the contract?	4	2	0	0
17	Do you implement measures to limit employees' administrative access to business (company) data specifically according to their job descriptions?	4	2	0	0
18	Do you always ensure that the firewall on your computer and/or laptop is always active to protect your important assets from cyber threats/attacks via the internet network?	4	2	0	0
19	Do you use passwords and encryption (eg WPA2-PSK) on your business (company) WiFi network?	4	2	0	0
20	Did you install the antivirus and set the antivirus update automatically?	4	2	0	0
21	Do you make sure that the emails you receive are safe from hackers who want to gain access to your network (phishing emails)?	4	2	0	0
22	Have you monitored log activity (digital records) for accounts that access your system?	4	2	0	0
23	Do you have an action plan to deal with leakage, loss, or theft of important business (company) assets?	4	2	0	0
24	Do you perform regular backups to prevent important information from being lost due to malfunctions or operational errors?	4	2	0	0
25	Have you studied and shared information about the latest threats and methods of cyber attack against applications, computers, laptops, and/or	4	2	0	0

No	Question	Assessment Point			
		DM	DS	TD	TT
	smartphones with internal businesses (companies)?				

Tabel 1 menunjukkan rincian soal pada PAMAN KAMI. DM berarti pelaku UMKM telah menerapkan perlindungan data terkait keamanan informasi dan mendapatkan poin 4. Sedangkan DS berarti pelaku UMKM telah menerapkan beberapa perlindungan data terkait keamanan informasi dan mendapatkan poin 2. Kemudian, TD berarti pelaku UMKM tidak menerapkan informasi perlindungan keamanan dengan poin 0. Terakhir, TT berarti pelaku UMKM tidak mengetahui atau tidak memahami pelaksanaan perlindungan keamanan informasi dengan poin 0. Tidak ada pertanyaan yang mendapat skor 1 atau 3, karena setiap jawaban yang netral dan ragu-ragu hanya akan dijawab mencetak 0.

3.2 Verifikasi Hasil Penilaian Keamanan Informasi

Setelah menjawab pertanyaan *self-assessment*, pengusaha akan mendapatkan hasil keamanan informasi yang dimilikinya. Hasilnya antara lain informasi mengenai keamanan siber dan pemanfaatan teknologi informasi yang dimiliki pengguna, serta rekomendasi tindakan yang perlu dilakukan untuk meningkatkan keamanan informasi tersebut. Perhitungan hasil *self-assessment* ditentukan berdasarkan akumulasi rumus 1 dari poin-poin yang diperoleh sebagai berikut.

$$\text{Total Poin} = DM + DS + TD + TT \quad (1)$$

Total poin PAMAN KAMI yang diperoleh kemudian dibagi menjadi 5 jenis klasifikasi atau kategori yang dijelaskan pada Tabel 2.

Tabel 2. Kategorisasi Tingkat Keamanan Informasi

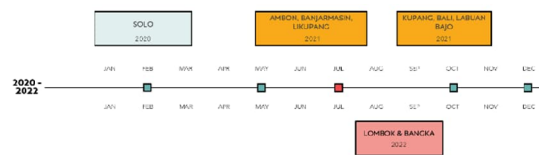
No	Category	Total Points	Notes
1	PERFECT	100	The implemented information security measures have been perfect. Do plan for additional security enhancements.
2	GOOD	90 - 99	Information security implementation is almost perfect and needs further security implementation.
3	ENOUGH	70 - 89	Implementation of information security is good enough and needs to increase protection measures.
4	LESS	50 - 69	The application of information security still has deficiencies in several fields.
5	BAD	< 50	Implemented information security can pose a potential risk from incidents of cyber attacks.

Dengan menggunakan PAMAN KAMI, pengguna dapat mengetahui tingkat keamanan siber

dan pemanfaatan teknologi informasi yang dimilikinya serta dapat meningkatkan kemampuan dan kinerjanya dalam menghadapi ancaman siber yang semakin kompleks dan beragam.

4. IMPLEMENTASI

Program dan metode PAMAN KAMI dilaksanakan dengan menggandeng pemerintah daerah dan berbagai pihak terkait untuk menilai kesadaran keamanan dan tingkat kematangan keamanan siber UMKM. Selain itu, BSSN menyelenggarakan seminar peningkatan *awareness* dan *cyber* literasi masyarakat Indonesia yang terbagi dalam 3 (tiga) tahun yaitu tahun 2020, 2021, dan 2022, dan dapat dilihat pada *timeline* pada Gambar 2.



Gambar 2. PAMAN KAMI implementation timeline

Gambar 2 tahapan penerapan PAMAN KAMI yang akan dilaksanakan pada tahun 2020 sebanyak 450 UMKM, tahun 2021 sebanyak 374 UMKM, dan tahun 2022 sebanyak 140 UMKM [14], [17] sampel yang lebih besar meningkatkan kekuatan statistik evaluasi. Riset [17] juga menunjukkan contoh berapa banyak peserta yang dikaitkan dengan *margin of error* dan populasi seperti terlihat pada Tabel 3. Penelitian ini menargetkan 1000 partisipan sehingga dapat mengambil kategori kolom 1 dengan *margin of error* 3%.

Tabel 3. Different-Sized Populations And Margin Of Errors

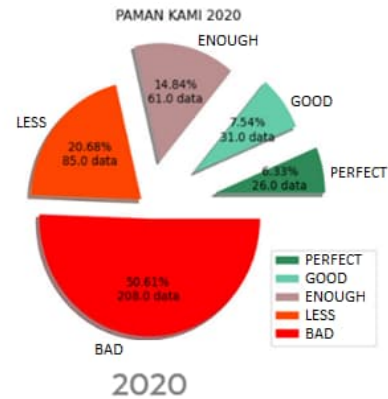
Popula- tion Size	Sample Size Based on $\pm 3\%$ Margin of Er- ror	Sample Size Based on $\pm 5\%$ Mar- gin of Error	Sample Size Based on $\pm 10\%$ Margin of Error
500	345	220	80
1000	525	285	90
3000	810	350	100
5000	910	370	100
10000	1000	385	100
10000+	1,100	400	100

5. HASIL DAN PEMBAHASAN

5.1 Hasil PAMAN KAMI

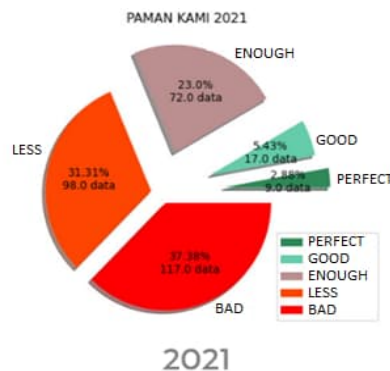
Pada tahun 2020, terdapat 450 UMKM di wilayah Solo yang hadir. Dari 450 UMKM, hanya 411 UMKM yang melakukan pengukuran menggunakan PAMAN KAMI seperti terlihat pada Gambar 3. Sebanyak 208 data memiliki kategori BURUK dengan persentase terbesar sekitar 50,61% menempati posisi pertama. Kategori KURANG berjumlah 85 data dengan persentase sekitar 20,68% pada posisi kedua dan kategori CUKUP berjumlah 61 data dengan persentase sekitar 14,48% pada posisi ketiga.

Sedangkan UMKM yang memiliki penilaian dengan kategori BAIK berjumlah 31 data dengan persentase sekitar 7,54% dan kategori SEMPURNA berjumlah 26 data dengan persentase sekitar 6,33%.



Gambar 3. PAMAN KAMI 2020 result

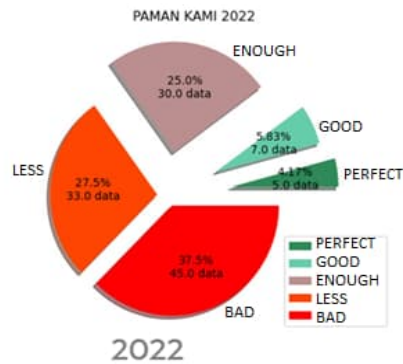
Pada tahun 2021, sebanyak 374 UMKM yang hadir, dan hanya 313 UMKM di wilayah Ambon, Banjarmasin, Likupang, Kupang, Bali, Labuan Bajo, Lombok, dan Bangka yang melakukan pengukuran menggunakan PAMAN KAMI seperti terlihat pada Gambar 4. Dari 313 UMKM tersebut, terdapat 117 data yang masuk dalam data PAMAN KAMI. Kategori BURUK dengan persentase terbesar yaitu sekitar 37,38% menempati posisi pertama. Kategori KURANG berjumlah 98 data dengan persentase sekitar 31,31% menempati posisi kedua dan kategori CUKUP berjumlah 72 data dengan persentase sekitar 23% menempati posisi ketiga. Sedangkan UMKM yang memiliki penilaian pada kategori BAIK berjumlah 17 data dengan persentase sekitar 5,43% dan kategori SEMPURNA berjumlah 9 data dengan persentase sekitar 2,88%.



Gambar 4. PAMAN KAMI 2021 result

Pada tahun 2022, dari 140 UMKM yang hadir, 120 UMKM di wilayah Ambon, Banjarmasin, Likupang, Kupang, Bali, Labuan Bajo, Lombok, dan Bangka melakukan pengukuran menggunakan PAMAN KAMI yang ditunjukkan pada Gambar 5. Dari 120 UMKM, 45 UMKM masuk dalam kategori BURUK dengan persentase terbesar sekitar 37,5% menempati posisi pertama. Kategori KURANG

berjumlah 33 data dengan persentase sekitar 27,5% menempati posisi kedua dan kategori CUKUP berjumlah 30 data dengan persentase sekitar 25% menempati posisi ketiga. Sedangkan UMKM yang memiliki penilaian pada kategori BAIK berjumlah 7 data dengan persentase sekitar 5,83% dan kategori SEMPURNA berjumlah 5 (lima) data dengan persentase sekitar 4,17%.



Gambar 5. PAMAN KAMI 2022 result

Penerapan PAMAN KAMI yang dibarengi dengan literasi keamanan siber di beberapa kota sangat penting untuk meningkatkan pemahaman terhadap ancaman dan solusi terhadap serangan yang dapat terjadi. Selain itu, di tengah meningkatnya jumlah pembobolan data dan pencurian identitas, keamanan data pribadi menjadi isu yang serius, PAMAN KAMI membantu mengidentifikasi dan memitigasi risiko kebocoran data pribadi, berkontribusi terhadap perlindungan hak privasi masyarakat Indonesia. Dengan menerapkan PAMAN KAMI, pemerintah dalam hal ini BSSN menunjukkan komitmennya dalam memberikan pemahaman tentang cara melindungi informasi pribadi dan sensitif warganya. Hal ini berdampak pada meningkatnya kepercayaan masyarakat terhadap instansi pemerintah dan pelayanan publik.

5.2 Rekomendasi

Dari keseluruhan hasil yang diperoleh selama 3 tahun terakhir program pembinaan PAMAN KAMI, hasil yang mendominasi adalah penilaian BURUK dan KURANG. Dapat diartikan bahwa *security awareness* dalam mengukur tingkat kematangan keamanan siber pada pengusaha UMKM belum optimal. BSSN dan berbagai pihak terkait perlu mendukung terciptanya keamanan informasi atau keamanan siber yang baik bagi UKM yang sudah menggunakan *platform online* dalam menjalankan usahanya, untuk mewujudkan keamanan nasional dan meningkatkan pertumbuhan ekonomi nasional.

6. KESIMPULAN

Penelitian ini menggunakan metode PAMAN KAMI untuk mengukur maturitas keamanan siber sektor UMKM. Kematangan dan kesadaran keamanan

diukur pada tahun 2020 – 2022 dengan total 964 UMKM yang berpartisipasi. Namun, hanya 844 UMKM yang melakukan pengukuran kesadaran dan kematangan keamanan siber secara mandiri.

Hasil yang mendominasi adalah BURUK dan KURANG sepanjang 3 (tiga) tahun terakhir. Dari pembahasan pengukuran kematangan dan kesadaran keamanan siber UMKM menggunakan PAMAN KAMI pada penelitian ini dapat disimpulkan bahwa:

1. PAMAN KAMI saat ini dapat dijadikan sebagai langkah awal bagi para pelaku UMKM untuk mengukur tingkat kesadaran dan keamanan informasinya sehingga risiko kejadian serangan siber dapat dicegah dan diminimalkan.
2. Perlunya koordinasi dan sinergi antara BSSN dengan Kementerian Koperasi dan Usaha Kecil Menengah (Kemenkop UKM) dan Kementerian Pariwisata dan Ekonomi Kreatif (Kemenparekraf) dalam membentuk ekosistem budaya keamanan siber yang kuat dan kokoh di Indonesia.

REFERENSI

- [1] ASEAN, "ASEAN Investment Report 2022 - Pandemic Recovery and Investment facilitation," 2022. [Online]. Available: <https://asean.org/book/asean-investment-report-2022/>
- [2] Kemenko Perekonomian, "Perkembangan UMKM sebagai Critical Engine Perekonomian Nasional Terus Mendapatkan Dukungan Pemerintah," 2022. [Online]. Available: www.ekon.go.id
- [3] Badan Pusat Statistik, "Pertumbuhan Ekonomi Indonesia Triwulan IV-2022," 2022. [Online]. Available: <https://www.bps.go.id/pressrelease/2020/02/05/1755/ekonomi-indonesia-2019-tumbuh-5-02-persen.html>
- [4] A. R. Yandwiputra and A. A. N. Hidayat, "Menteri Bahlil Catat Sektor UMKM Tahun 2022 Serap Tenaga Kerja 7 Juta Orang," *Bisnis Tempo.co*, 2023. <https://bisnis.tempo.co/read/1688395/menteri-bahlil-catat-sektor-umkm-tahun-2022-serap-tenaga-kerja-7-juta-orang> (accessed Apr. 16, 2023).
- [5] M. S. Umam, "Orientasi Etika dan Cyber Security Awareness (Studi Kasus pada UMKM di Bantul)," *Akmenika J. Akunt. dan Manaj.*, vol. 13, no. 2, pp. 283–291, 2019, doi: 10.31316/akmenika.v16i2.394.
- [6] G. D. Rahmadiane, E. Unggul, S. Utami, and T. Anggraeni, "Analisis Pertumbuhan Startup Bisnis di Kota Tegal," *Manag. Insight J. Ilm. Manaj.*, vol. 17, no. 2, pp. 152–160, 2022.

- [7] T. Nuryati, D. Puspaningtyas, F. Nabilla, and E. Teguh, "Digital Transformation , Work From Home On The Performance Of Culinary M SMES In Indonesia After The Pandemic," vol. 3, no. 1, pp. 520–540, 2023.
- [8] F. X. K. Tjakrawala and J. Iskak, "Edukasi Aspek Keamanan Dan Pengendalian Data Guna Membangun Literasi Digital Bagi Pelaku Umkm," *Pros. SENAPENMAS*, p. 321, 2021, doi: 10.24912/psenapenmas.v0i0.15005.
- [9] I. M. Suartana, R. Eka Putra, R. Bisma, and A. Prapanca, "Pengenalan Pentingnya Cyber Security Awareness pada UMKM," *J. Abadimas Adi Buana*, vol. 5, no. 02, pp. 197–204, 2022, doi: 10.36456/abadimas.v5.i02.a4560.
- [10] Y. A. Singgalen, H. D. Purnomo, and I. Sembiring, "Exploring MSMEs Cybersecurity Awareness and Risk Management: Information Security Awareness ," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 15, no. 3, p. 233, 2021, doi: 10.22146/ijccs.67010.
- [11] A. Zamsuri, W. Syafitri, and E. Syahputra Pane, "Evaluation of Information Security Awareness on Digital Marketing (Case Study of MSME in Indonesia)," vol. 2, no. 1, pp. 192–210, 2021, [Online]. Available: <https://doi.org/10.30880/ahcs.2021.02.01.020>
- [12] Badan Standarisasi Nasional Indonesia, "Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Persyaratan (ISO/IEC 27001:2013, IDT)," 2016
- [13] A. A. Wardana, "Evaluation of Information Security Management in Micro , Small , and Medium Enterprises (MSMEs) using Penilaian Mandiri Keamanan Informasi (PAMAN KAMI)," 2023.
- [14] B. N. Kantharia, "S Ix Rules of Thum B for De Ter M Ining S a M Ple S Ize a Nd S Tatis Tic a L Pow Er Six Rules of Thumb for Deter Mining S a M P L E S I Z E a N D S Tat I S T I C a L P Ow E R," *Manag. Sci.*, vol. 1, 1997.
- [15] R. Kissel, "Small Business Information Security : The Fundamentals Small Business Information Security : The Fundamentals," *Natl. Inst. Stand. Technol. Interag. Rep.*, vol. 7621, p. 20, 2016.
- [16] S. Pawar and D. H. Palivela, "LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)," *Int. J. Inf. Manag. Data Insights*, vol. 2, no. 1, p. 100080, 2022, doi: 10.1016/j.jjimei.2022.100080.
- [17] M. Brysbaert, "How many participants do we have to include in properly powered experiments? A tutorial of power analysis with reference tables," *J. Cogn.*, vol. 2, no. 1, 2019, doi: 10.5334/JOC.72/.