JABA (Maret 2022)
Journal of Applied Business Administration
https://jurnal.polibatam.ac.id

ANALISIS PENILAIAN KEAMANAN INFORMASI DENGAN MENGGUNAKAN PENILAIAN MANDIRI KEAMANAN INFORMASI (PAMAN KAMI)

Muhammad Ramadhan Slamet [1)]✉, Muhammad Ikhlash [2)]✉, Febrina Wulandari[3)]✉

Jurusan Manajemen Bisnis, Politeknik Negeri Batam

Info Artikel

Diserahkan Nov 2021
Diterima Feb 2022
Diterbitkan Maret 2022

Kata Kunci:
PAMAN KAMI, UKM, Keamanan Informasi

Abstrak

Sebagai bentuk upaya mitigasi, para pelaku UKM dapat menggunakan PAMAN KAMI, termasuk diantaranya adalah unit-unit usaha yang ada di lingkungan Universitas XYZ, yaitu PT A, Koperasi B, dan Penerbitan C. Tujuan penelitian ini adalah untuk mengidentifikasi sejauh mana level keamanan informasi pada PT "A", Koperasi "B", dan Penerbit "C". Metode penelitian yang digunakan adalah penelitian kuantitatif deskriptif. Metode tersebut digunakan karena dapat mendeskripsikan sejauh mana level keamanan informasi pada PT "A", Koperasi "B", dan Penerbit "C". Teknik pengambilan sampel yang digunakan pada penelitian ini ialah pengambilan sampel berdasarkan pertimbangan tertentu (judgement sampling). Teknik pengumpulan data yang digunakan dalam penelitian ini, yaitu kuesioner. Hasil dari penilaian menunjukkan bahwasanya PT "A" mendapatkan skor 38 yang artinya level keamanan informasinya masuk ke dalam kategori buruk. Sementara itu, Koperasi "B" mendapatkan skor 52 yang artinya level keamanan informasinya masuk ke dalam kategori kurang. Terakhir, Penerbit "C" mendapatkan skor 54 yang artinya level keamanan informasinya masuk ke dalam kategori kurang. Berdasarkan hal tersebut dapat disimpulkan bahwa level keamanan informasi untuk ketiganya masih di bawah dari level cukup. Hal tersebut disebabkan karena fokus ketiganya masih bersifat operasional dan belum berfokus ke arah strategis (seperti keamanan informasi).

✉ Alamat Korespondensi:
Jurusan Manajemen Bisnis
Politeknik Negeri Batam
E-mail: ramadhanslamet@polibatam.ac.id

ISSN 2548-9909

1. Pendahuluan

Tahun 2020 merupakan suatu momentum dimana hampir semua lapisan masyarakat menggunakan internet. Hal tersebut didorong karena pandemi Covid-19 sehingga terjadi peningkatan dalam jumlah pengguna internet. Berdasarkan hasil survei yang telah dilakukan oleh APJII 2019-2020Q2, jumlah pengguna internet di Indonesia meningkat 8,9% dibandingkan tahun 2018 menjadi 196,7 juta.

Peningkatan jumlah pengguna internet tersebut mengindikasikan bahwa dunia maya tidak hanya dihuni oleh masyarakat yang paham teknologi, tetapi juga dihuni oleh masyarakat yang masih awam dengan teknologi. Hal tersebut menimbulkan adanya celah terjadinya serangan siber. Berdasarkan hasil monitong keamanan siber dari BSSN (2020) telah terjadi kasus kebocoran data terbesar yang dialami oleh salah satu e-commerce terbesar di Indonesia, yaitu Tokopedia. Setidaknya, terdapat 91 juta data yang bocor di internet berupa identitas pengguna.

Kasus siber tidak hanya dialami oleh perusahaan besar, tetapi juga dapat dialami oleh para pelaku Usaha Kecil Menengah (UKM). Menurut Annur (2020) perusahaan Kapersky telah memeriksa ribuan serangan yang ditujukan ke UKM kawasan Asia Tenggara pada triwulan I 2020. Hasilnya, terdapat 192 ribu serangan berupa phising yang ditujukan ke UKM di Indonesia. Hal tersebut dikarenakan para karyawan UKM yang bekerja dari rumah kurang dilengkapi sistem keamanan yang baik selama awal pandemi.

Terdapat beberapa *framework* yang dapat digunakan untuk mengevaluasi keamanan informasi pada UKM. Pada penelitian Alshboul dan Streff (2015) membuat suatu kerangka kerja (*framework*) keamanan informasi bagi UKM. *Framework* yang dijadikan dasar dalam penelitiannya adalah Plan, Do, Check, Act (PDCA) dan NIST 6721. Sementara itu, Fauzi (2018) berfokus pada implementasi keamanan informasi pada salah satu UKM yang bergerak di bidang *engineering servies*. *Framework* yang digunakan adalah ISO/IEC 27001. Selain itu, digunakan juga metode OCTAVE untuk menganalisis risiko. Terakhir, Ozkan, dkk (2020) membuat suatu metode dalam implementasi keamanan informasi sesuai karakteristik organisasi. Penelitian ini berfokus pada UKM. *Framework* yang digunakan adalah ISFAM Model.

Guna mencegah kerugian sejak dini pada pelaku UKM di Indonesia, diperlukan langkah perlindungan melalui pemahaman terkait keamanan informasi. Oleh sebab itu, Badan Siber dan Sandi Negara (BSSN) mengeluarkan Penilaian Mandiri Keamanan Informasi atau disingkat dengan PAMAN KAMI. Penilaian tersebut merupakan langkah awal dalam memeriksa status keamanan informasi UKM. Harapannya, para pelaku UKM dapat melakukan pencegahan terjadinya serangan siber melalui penyusunan strategi sampai dengan penanggulangan ketika terjadi serangan tersebut.

Menurut BSSN (2020), syarat UKM yang dapat menggunakan PAMAN KAMI, yaitu tidak memiliki server atau peralatan jaringan yang rumit dan hanya menggunakan aplikasi komersial dari pihak ketiga. Unit-unit usaha yang ada di lingkungan Universitas XYZ, yaitu PT "A", Koperasi "B", dan Penerbit "C" dapat menggunakan PAMAN KAMI karena sesuai dengan syarat yang ditetapkan oleh BSSN. Terlebih, Universitas XYZ pernah mengalami serangan siber pada tahun 2021 sehingga penting bagi unit-unit usahanya untuk melakukan mitigasi terkait keamanan informasi.

Unit-unit usaha tersebut belum pernah mengecek status keamanan informasi usahanya dengan menggunakan PAMAN KAMI. Oleh sebab itu, terdapat celah antara kondisi sebenarnya dan kondisi ideal. Berdasarkan hal tersebut, pertanyaan penelitian yang diusulkan adalah sejauh mana level keamanan informasi pada PT "A", Koperasi "B", dan Penerbit "C". Tujuan penelitian ini adalah untuk mengidentifikasi sejauh mana level keamanan informasi pada PT "A", Koperasi "B", dan Penerbit "C".

2. Metode

2.1 Teknik Penentuan Sampel

Pada penelitian ini teknik penentuan sampel yang digunakan adalah *judgement sampling*. Menurut Sudaryono (2021), teknik

sampel ini didasarkan atas pertimbangan tertentu. Berdasarkan panduan Penilaian Mandiri Keamanan Informasi (PAMAN KAMI) versi 2.0 yang dikerluarkan oleh BSSN (2020), pihak yang menjadi responden dalam penelitian ini diprioritaskan merupakan pimpinan atau manajer usaha ataupun karyawan yang memahami terkait keamanan informasi di perusahaannya. Pada penelitian ini terdiri dari 3 (tiga) orang responden, yaitu 1 (satu) orang dari pimipinan PT "A", 1 (satu) orang pimpinan dari Koperasi "B", dan 1 (orang) karyawan dari Penerbit "C". Alasan dipilihnya responden tersebut karena responden memiliki pengetahuan terkait keamanan informasi yang dilaksanakan pada unit usahanya.

2.2 Teknik Pengumpulan Data

Pada penelitian ini akan dilakukan teknik pengumpulan data berupa kuesioner. Kuesioner dalam penelitian ini diadopsi dari Penilaian Mandiri Keamanan Informasi (PAMAN KAMI) versi 2.0. Kuesioner terbagi menjadi dua bagian, yaitu identifikasi responden dan pertanyaan keamanan informasi sebanyak 25 pertanyaan.

2.3 Tahap Penilaian

a. Responden mengisi identifikasi responden dan daftar pertanyaan terkait keamanan informasi yang telah berjalan. Pertanyaan ini didasarkan atas PAMAN KAMI versi 2.0 yang berfokus pada 25 langkah keamanan informasi. Pada setiap pertanyaan, akan ada pilihan jawaban DM, DS, TD, dan TT.
    1) DM (Diterapkan Menyeluruh). Artinya, jika item penilaian diterapkan secara menyeluruh terhadap seluruh karyawan baik pribadi maupun organisasi. Skornya bernilai 4.
    2) DS (Diterapkan Sebagian). Artinya, jika item penilaian hanya diterapkan oleh sebagian dari karyawan atau organisasi. Skornya bernilai 2.
    3) TD (Tidak Diterapkan). Artinya, jika item penilaian belum diterapkan sama sekali oleh karyawan maupun organisasi. Skornya bernilai 0.
    4) TT (Tidak Tahu). Artinya, jika Anda belum memahami item penilaian tersebut. Skornya bernilai 0.
b. Peneliti melakukan *scoring* yang ditentukan dari Total DM + Total DS. Berikut hasilnya.

Jika Anda mencetak 100 poin **(SEMPURNA)**	Langkah keamanan informasi yang Anda terapkan sudah sempurna. Rencanakan langkah untuk naik ke level berikutnya.
Jika Anda mencetak 90-99 poin **(BAIK)**	Hampir sempurna, namun ada beberapa langkah yang belum diterapkan secara menyeluruh, sehingga butuh penerapan keamanan lebih lanjut.
Jika Anda mencetak 70-89 poin **(CUKUP)**	Langkah keamanan cukup baik. Terapkan langkah proteksi yang ada untuk meningkatkan keamanan informasi Anda.
Jika Anda mencetak 50 - 69 poin **(KURANG)**	Terdapat bidang yang secara eksplisit mengalami kekurangan langkah keamanan.
Jika Anda mencetak 49 poin atau lebih rendah **(BURUK)**	Keamanan informasi perusahaan Anda buruk. Anda seharusnya tidak terkejut jika terjadi insiden seperti kebocoran data.

Gambar. 1. Skor Penilaian Mandiri Kemanan Informasi (PAMAN KAMI)
Sumber: BSSN (2020)

c. Peneliti mengkaji hasil PAMAN KAMI. Pengkajian didasarkan atas hasil perhitungan skor. Selain itu, akan diberikan rekomendasi berdasarkan hasilnya.

3. Hasil dan Pembahasan

3.1 Pengisian Kuesioner

Kuesioner diisi oleh masing-masing responden yang dipandu oleh peneliti melalui *zoom meeting* sehingga responden paham apa yang dimaksud dari setiap pertanyaan baik identitas usaha dan pertanyaan keamanan informasi. Setelah diisi, peneliti melakukan identifikasi profil usaha, dan melakukan *scoring* serta pengkajian hasil berdasarkan hasil kuesioner.

3.2 Identifikasi Profil Usaha

Berdasarkan skala usaha, ketiganya termasuk katergori skala usaha kecil. Sementara berdasarkan bentuk usaha, masing-masing memiliki bentuk yang berbeda-beda. PT "A" merupakan bentuk usaha perseroan terbatas (PT). Koperasi "B" merupakan bentuk usaha koperasi, sedangkan Penerbit "C" merupakan bentuk usaha unit bisnis dari Universitas XYZ. PT "A" dan Koperasi "B" memiliki aset usaha yang sama, yaitu 50 – 500 juta. Sementara itu,

Penerbit "C" memiliki aset usaha < 50 juta. Jika didasarkan atas omzet usaha, Koperasi "B" dan Penerbit "C" memiliki omzet usaha yang sama, yaitu < 300 juta. PT "A" memiliki omzet usaha 300 juta – 2,5 miliar. Berdasarkan jumlah karyawan, ketiganya memiliki jumlah karyawan yang sama, yaitu < 10 orang.

Ketiganya menggunakan media sosial. Platform yang digunakan ada yang sama dan ada yang berbeda. Whatsapp merupakan platform yang digunakan oleh ketiganya. Instagram digunakan oleh Penerbit "C" dan PT "A", sedangkan Facebook hanya digunakan oleh Penerbit "C". Jika didasarkan atas marketplace, hanya Penerbit "C" yang menggunakannya. Hal yang sama terkait dengan website pribadi. Hanya Penerbit "C" yang memiliki website pribadi. Terkait dengan mobile apps, ketiganya menggunakan mobile banking. PT "A" dan Penerbit "C" menggunakan mobile banking dari BSI, sedangkan Koperasi "B" menggunakan mobile banking dari BNI. Selain mobile banking, ada juga aplikasi lain yang digunakan, seperti Canva (PT "A"), dan Olsera serta Deskera (Koperasi "B"). Penjelasan tersebut dapat dilihat pada tabel 1.

Tabel 1 Profil Identitas Usaha

No	Aspek	PT "A"	Koperasi "B"	Penerbit "C"
1.	Skala Usaha	Kecil	Kecil	Kecil
2.	Bentuk Usaha	PT	Koperasi	Unit Bisnis
3.	Aset Usaha	50 - 500 juta	50 - 500 juta	< 50 juta
4.	Omzet Usaha	300 juta - 2,5 miliar	< 300 juta	< 300 juta
5.	Jumlah Karyawan	< 10 orang	< 10 orang	< 10 orang
6.	Media Sosial	Instagram dan Whatsapp	Whatsapp	Facebook, Instagram, dan Whatsapp
7.	Marketplace	(Tidak Ada)	(Tidak Ada)	Bukalapak, Blibli, Lazada, dan Google Books
8.	Website Pribadi	(Tidak Ada)	(Tidak Ada)	(Ada)
9.	Mobile Apps	Mobile Banking dan Canva	Mobile Banking, Olsera, Deskera	Mobile Banking

Keterangan: Hasil Kuesioner

3.2 *Scoring* dan Pengkajian Hasil

A. PT "A"

Tabel 2 menunjukkan penilaian keamanan informasi di PT "A". Berdasarkan penilaian, kategori keamanan PT "A" masuk ke kategori buruk. Hal ini mengindikasikan jika PT "A" rentan terjadi insiden kebocoran data. Hasil penilaian ini dapat dimaklumi karena fokus PT "A" masih bersifat operasional dan belum sepenuhnya berfokus ke sisi strategis (seperti keamanan informasi).

Tabel 2 Penilaian Keamanan Informasi PT "A"

No	Jawaban	Jumlah Pertanyaan	Skor (Jawaban x Jumlah Pertanyaan)
1	Diterapkan Menyeluruh (4 poin)	6	24
2	Diterapkan Sebagian (2 poin)	7	14
3	Tidak Diterapkan (0 poin)	12	0
4	Tidak Tahu (0 poin)	0	0
	Total	25	38
		Katergori	**Buruk**

Kategori Skor: 100 : Sempurna; 90-99 : Baik; 70-89 : Cukup; 50-69 : Kurang; >49 : Buruk

Keterangan: Hasil Kuesioner

Terdapat 6 bentuk keamanan informasi yang telah dilakukan secara menyeluruh, yaitu.

1) Menerapkan penggunaan kata sandi (password) pada perangkat komputer, laptop dan/atau smartphone untuk mencegah pencurian data
2) Membuat kata sandi (password) yang kuat dan tidak mudah ditebak serta tidak menggunakan kata sandi yang sama untuk beberapa Akun (layanan web)
3) Saat melihat ada orang yang tidak dikenal memasuki area kerja terbatas milik usaha (perusahaan), Usaha/Perusahaan melakukan pengamanan dengan cara mendekati dan menanyakan maksud dan tujuan kedatangan orang tersebut
4) Selalu menjaga Operating System, smartphone, perangkat lunak dan aplikasi usaha (perusahaan) mendapatkan pembaruan (update) keamanan dari vendor/penyedia secara otomatis
5) Mewajibkan mitra bisnis untuk menjaga kerahasiaan, seperti menyertakan klausul kerahasiaan (kewajiban untuk menjaga kerahasiaan) dalam kontrak
6) Selalu memastikan bahwa firewall pada komputer dan/atau laptop selalu aktif dengan tujuan untuk melindungi aset penting Usaha/Perusahaan dari ancaman/serangan siber melalui jaringan internet

Terdapat 7 bentuk keamanan informasi yang telah diterapkan sebagian, yaitu.

1) Melakukan identifikasi terhadap aset-aset penting usaha (perusahaan) yang harus dilindungi
2) Menerapkan langkah untuk mencegah hilang atau bocornya informasi penting, seperti menyimpan informasi penting di kabinet/lemari/laci yang terkunci, dan tidak meninggalkannya di atas meja
3) Menerapkan kebijakan tidak menghubungkan komputer, laptop, dan smartphone Usaha/Perusahaan dengan jaringan internet (Wi- Fi) publik pada saat mengakses akun-akun penting
4) Menerapkan langkah untuk membatasi akses administratif karyawan terhadap data usaha (perusahaan) secara spesifik sesuai dengan deskripsi tugasnya
5) Menerapkan penggunaan kata sandi (password) dan enkripsi (misal: WPA2-PSK) pada jaringan WiFi milik usaha (perusahaan) Usaha/Perusahaan
6) Menginstal antivirus dan mengatur pembaruan antivirus secara otomatis
7) Melakukan pencadangan rutin guna mencegah agar informasi penting tidak hilang karena kegagalan fungsi atau kesalahan operasi

Terdapat 12 bentuk keamanan informasi yang tidak diterapkan, yaitu.

1) Melakukan identifikasi terhadap semua kemungkinan risiko hilangnya aset-aset penting usaha (perusahaan)
2) Memiliki prosedur dan kebijakan keamanan informasi yang diterapkan untuk melindungi aset-aset penting usaha (perusahaan)
3) Memasang alat elektronik anti petir (Surge Protector) dan Uninterruptible Power Supplies (UPS) yang digunakan untuk melindungi perangkat jaringan usaha (perusahaan) dari sambaran petir, lonjakan listrik atau hubungan pendek listrik
4) Saat membuang/menghapus informasi penting, Usaha/Perusahaan memastikan bahwa informasi penting yang dibuang/dihapus menjadi tidak terbaca lagi, seperti menggunakan penghancur kertas/alat penghapus data
5) Menerapkan cara untuk menghindari serangan rekayasa sosial (social engineering) seperti membatasi informasi pribadi yang dibagikan kepada publik atau bersikap skeptis terhadap orang tidak dikenal yang ingin mengetahui informasi sensitif Usaha/Perusahaan
6) Selalu memastikan bahwa aplikasi yang Usaha/Perusahaan unduh dan instal pada komputer, laptop, dan smartphone usaha (perusahaan) aman dan berasal dari sumber tepercaya

7) Menerapkan kebijakan untuk mengontrol penggunaan Internet, seperti menetapkan aturan tentang menjelajahi situs web dan mengunggah ke media sosial di komputer area kerja (kantor)
8) Mempunyai program untuk memberikan pemahaman kepada karyawan akan pentingnya keamanan informasi dan bahwa keamanan informasi merupakan tanggung jawab semua orang yang bekerja pada usaha (perusahaan)
9) Memastikan bahwa email yang Usaha/Perusahaan terima aman dari peretas yang ingin mendapatkan akses ke jaringan Usaha/Perusahaan (email phishing)
10) Melakukan pemantauan aktivitas log (catatan digital) terhadap akun yang melakukan akses terhadap sistem Usaha/Perusahaan
11) Memiliki rencana tindak untuk menangani kebocoran, kehilangan, atau pencurian aset penting usaha (perusahaan)
12) Mempelajari dan membagikan informasi tentang ancaman dan metode serangan siber terbaru terhadap aplikasi, komputer, laptop, dan/atau smartphone kepada internal usaha (perusahaan)

B. Koperasi "B"

Tabel 3 menunjukkan penilaian keamanan informasi di Koperasi "B". Berdasarkan penilaian, kategori keamanan Koperasi "B" masuk ke kategori kurang. Hal ini mengindikasikan jika terdapat bidang yang secara eksplisit kekurangan langkah keamanan. Hasil penilaian ini dapat dimaklumi karena fokus Koperasi "B" masih bersifat operasional dan belum sepenuhnya berfokus ke sisi strategis (seperti keamanan informasi).

Tabel 2 Penilaian Keamanan Informasi Koperasi "B"

No	**Jawaban**	**Jumlah Pertanyaan**	**Skor (Jawaban x Jumlah Pertanyaan)**
1	Diterapkan Menyeluruh (4 poin)	9	36
2	Diterapkan Sebagian (2 poin)	8	16
3	Tidak Diterapkan (0 poin)	7	0
4	Tidak Tahu (0 poin)	1	0
	Total	25	52
		Katergori	**Kurang**

Kategori Skor: 100 : Sempurna; 90-99 : Baik; 70-89 : Cukup; 50-69 : Kurang; >49 : Buruk

Keterangan: Hasil Kuesioner

Terdapat 9 bentuk keamanan informasi yang telah dilakukan secara menyeluruh, yaitu.

1) Saat melihat ada orang yang tidak dikenal memasuki area kerja terbatas milik usaha (perusahaan), Usaha/Perusahaan melakukan pengamanan dengan cara mendekati dan menanyakan maksud dan tujuan kedatangan orang tersebut
2) Saat membuang/menghapus informasi penting, Usaha/Perusahaan memastikan bahwa informasi penting yang dibuang/dihapus menjadi tidak terbaca lagi, seperti menggunakan penghancur kertas/alat penghapus data
3) menerapkan cara untuk menghindari serangan rekayasa sosial (social engineering) seperti membatasi informasi pribadi yang dibagikan kepada publik atau bersikap skeptis terhadap orang tidak dikenal yang ingin mengetahui informasi sensitif Usaha/Perusahaan
4) Mewajibkan mitra bisnis untuk menjaga kerahasiaan, seperti menyertakan klausul kerahasiaan (kewajiban untuk menjaga kerahasiaan) dalam kontrak
5) Menerapkan langkah untuk membatasi akses administratif karyawan terhadap data usaha (perusahaan) secara spesifik sesuai dengan deskripsi tugasnya

6) Menerapkan penggunaan kata sandi (password) dan enkripsi (misal: WPA2-PSK) pada jaringan WiFi milik usaha (perusahaan) Usaha/Perusahaan
7) Menginstal antivirus dan mengatur pembaruan antivirus secara otomatis
8) Memastikan bahwa email yang Usaha/Perusahaan terima aman dari peretas yang ingin mendapatkan akses ke jaringan Usaha/Perusahaan Anda (email phishing)
9) Memiliki rencana tindak untuk menangani kebocoran, kehilangan, atau pencurian aset penting usaha (perusahaan)

Terdapat 8 bentuk keamanan informasi yang telah dilakukan sebagian, yaitu.

1) Melakukan identifikasi terhadap aset-aset penting usaha (perusahaan) yang harus dilindungi
2) Menerapkan penggunaan kata sandi (password) pada perangkat komputer, laptop dan/atau smartphone untuk mencegah pencurian data
3) Membuat kata sandi (password) yang kuat dan tidak mudah ditebak serta tidak menggunakan kata sandi yang sama untuk beberapa Akun (layanan web)
4) Menerapkan langkah untuk mencegah hilang atau bocornya Informasi penting, seperti menyimpan informasi penting di kabinet/lemari/laci yang terkunci, dan tidak meninggalkannya di atas meja
5) Memasang alat elektronik anti petir (Surge Protector) dan Uninterruptible Power Supplies (UPS) yang digunakan untuk melindungi perangkat jaringan usaha (perusahaan) dari sambaran petir, lonjakan listrik atau hubungan pendek listrik
6) Selalu menjaga Operating System, smartphone, perangkat lunak dan aplikasi usaha (perusahaan) mendapatkan pembaruan (update) keamanan dari vendor/penyedia secara otomatis
7) Selalu memastikan bahwa aplikasi yang Usaha/Perusahaan unduh dan instal pada komputer, laptop, dan smartphone usaha (perusahaan) aman dan berasal dari sumber tepercaya
8) Melakukan pencadangan rutin guna mencegah agar informasi penting tidak hilang karena kegagalan fungsi atau kesalahan operasi

Terdapat 7 bentuk keamanan informasi yang tidak diterapkan, yaitu.

1) Melakukan identifikasi terhadap semua kemungkinan risiko hilangnya aset-aset penting usaha (perusahaan)
2) Memiliki prosedur dan kebijakan keamanan informasi yang diterapkan untuk melindungi aset-aset penting usaha (perusahaan)
3) Menerapkan kebijakan tidak menghubungkan komputer, laptop, dan smartphone Usaha/Perusahaan dengan jaringan internet (Wi- Fi) publik pada saat mengakses akun-akun penting
4) Menerapkan kebijakan untuk mengontrol penggunaan Internet, seperti menetapkan aturan tentang menjelajahi situs web dan mengunggah ke media sosial di komputer area kerja (kantor)
5) Mempunyai program untuk memberikan pemahaman kepada karyawan akan pentingnya keamanan informasi dan bahwa keamanan informasi merupakan tanggung jawab semua orang yang bekerja pada usaha (perusahaan)
6) Melakukan pemantauan aktivitas log (catatan digital) terhadap akun yang melakukan akses terhadap sistem Usaha/Perusahaan
7) Mempelajari dan membagikan informasi tentang ancaman dan metode serangan siber terbaru terhadap aplikasi, komputer, laptop, dan/atau smartphone kepada internal usaha (perusahaan)

Terdapat 1 bentuk keamanan informasi yang tidak diketahui, yaitu "Selalu memastikan bahwa firewall pada komputer dan/atau laptop selalu aktif dengan tujuan untuk melindungi aset penting Usaha/Perusahaan dari ancaman/serangan siber melalui jaringan internet".

B. Penerbit "C"

Tabel 4 menunjukkan penilaian keamanan informasi di Penerbit "C". Berdasarkan penilaian, kategori keamanan Penerbit "C" masuk ke kategori kurang. Hal ini mengindikasikan jika terdapat bidang yang secara eksplisit kekurangan langkah keamanan. Hasil penilaian ini dapat dimaklumi karena fokus dan usia Penerbit "C" masih bersifat operasional dan belum sepenuhnya berfokus ke sisi strategis (seperti keamanan informasi).

Tabel 3 Penilaian Keamanan Informasi Penerbit "C"

No	Jawaban	Jumlah Pertanyaan	Skor (Jawaban x Jumlah Pertanyaan)
1	Diterapkan Menyeluruh (4 poin)	8	32
2	Diterapkan Sebagian (2 poin)	11	22
3	Tidak Diterapkan (0 poin)	6	0
4	Tidak Tahu (0 poin)	0	0
	Total	25	54
		Katergori	**Kurang**

Kategori Skor: 100 : Sempurna; 90-99 : Baik; 70-89 : Cukup; 50-69 : Kurang; >49 : Buruk

Keterangan: Hasil Kuesioner

Terdapat 8 bentuk keamanan informasi yang telah diterapkan secara menyeluruh, yaitu.

1. Membuat kata sandi (password) yang kuat dan tidak mudah ditebak serta tidak menggunakan kata sandi yang sama untuk beberapa Akun (layanan web)
2. menerapkan langkah untuk mencegah hilang atau bocornya Informasi penting, seperti menyimpan informasi penting di kabinet/lemari/laci yang terkunci, dan tidak meninggalkannya di atas meja
3. Saat melihat ada orang yang tidak dikenal memasuki area kerja terbatas milik usaha (perusahaan), Usaha/Perusahaan melakukan pengamanan dengan cara mendekati dan menanyakan maksud dan tujuan kedatangan orang tersebut
4. Selalu memastikan bahwa aplikasi yang Usaha/Perusahaan unduh dan instal pada komputer, laptop, dan smartphone usaha (perusahaan) aman dan berasal dari sumber tepercaya
5. Mewajibkan mitra bisnis untuk menjaga kerahasiaan, seperti menyertakan klausul kerahasiaan (kewajiban untuk menjaga kerahasiaan) dalam kontrak
6. Menerapkan langkah untuk membatasi akses administratif karyawan terhadap data usaha (perusahaan) secara spesifik sesuai dengan deskripsi tugasnya
7. Memastikan bahwa email yang Usaha/Perusahaan terima aman dari peretas yang ingin mendapatkan akses ke jaringan Usaha/Perusahaan Anda (email phishing)
8. Melakukan pencadangan rutin guna mencegah agar informasi penting tidak hilang karena kegagalan fungsi atau kesalahan operasi

Terdapat 11 bentuk keamanan informasi yang telah dilakukan sebagian, yaitu.

1. Melakukan identifikasi terhadap aset-aset penting usaha (perusahaan) yang harus dilindungi
2. Melakukan identifikasi terhadap semua kemungkinan risiko hilangnya aset-aset penting usaha (perusahaan)
3. Menerapkan penggunaan kata sandi (password) pada perangkat komputer, laptop dan/atau smartphone untuk mencegah pencurian data
4. Memasang alat elektronik anti petir (Surge Protector) dan Uninterruptible Power Supplies (UPS) yang digunakan untuk melindungi perangkat jaringan usaha (perusahaan) dari sambaran petir,

lonjakan listrik atau hubungan pendek listrik
5. Saat membuang/menghapus informasi penting, Usaha/Perusahaan memastikan bahwa informasi penting yang dibuang/dihapus menjadi tidak terbaca lagi, seperti menggunakan penghancur kertas/alat penghapus data
6. Selalu menjaga Operating System, smartphone, perangkat lunak dan aplikasi usaha (perusahaan) mendapatkan pembaruan (update) keamanan dari vendor/penyedia secara otomatis
7. Menerapkan kebijakan untuk mengontrol penggunaan Internet, seperti menetapkan aturan tentang menjelajahi situs web dan mengunggah ke media sosial di komputer area kerja (kantor)
8. Selalu memastikan bahwa firewall pada komputer dan/atau laptop selalu aktif dengan tujuan untuk melindungi aset penting Usaha/Perusahaan Anda dari ancaman/serangan siber melalui jaringan internet
9. Menerapkan penggunaan kata sandi (password) dan enkripsi (misal: WPA2-PSK) pada jaringan WiFi milik usaha (perusahaan) Usaha/Perusahaan Anda
10. Menginstal antivirus dan mengatur pembaruan antivirus secara otomatis
11. 1Melakukan pemantauan aktivitas log (catatan digital) terhadap akun yang melakukan akses terhadap sistem Usaha/Perusahaan

Terdapat 6 bentuk keamanan informasi yang tidak diterapkan, yaitu.

1. Memiliki prosedur dan kebijakan keamanan informasi yang diterapkan untuk melindungi aset-aset penting usaha (perusahaan)
2. Menerapkan kebijakan tidak menghubungkan komputer, laptop, dan smartphone Usaha/Perusahaan dengan jaringan internet (Wi- Fi) publik pada saat mengakses akun-akun penting
3. Menerapkan cara untuk menghindari serangan rekayasa sosial (social engineering) seperti membatasi informasi pribadi yang dibagikan kepada publik atau bersikap skeptis terhadap orang tidak dikenal yang ingin mengetahui informasi sensitif Usaha/Perusahaan
4. Mempunyai program untuk memberikan pemahaman kepada karyawan akan pentingnya keamanan informasi dan bahwa keamanan informasi merupakan tanggung jawab semua orang yang bekerja pada usaha (perusahaan)
5. Memiliki rencana tindak untuk menangani kebocoran, kehilangan, atau pencurian aset penting usaha (perusahaan)
6. Mempelajari dan membagikan informasi tentang ancaman dan metode serangan siber terbaru terhadap aplikasi, komputer, laptop, dan/atau smartphone kepada internal usaha (perusahaan)

4. Kesimpulan

Menurut panduan Penilaian Mandiri Keamanan Informasi (PAMAN KAMI) versi 2.0 yang dikerluarkan oleh BSSN (2020), jika mendapatkan skor penilaian 100, akan masuk ke kategori sempurna. Jika mendapatkan skor penilaian 90 sampai 99, akan masuk ke kategori baik. Kemudian, jika mendapatkan skor penilaian 70 sampai 89, akan masuk ke kategori cukup. Sementara, jika mendapatkan skor penilaian 50 sampai 69, akan masuk ke kategori kurang. Terakhir, jika mendapatkan skor penilaian kurang dari 49, akan masuk ke kategori buruk.

Hasil dari penilaian menunjukkan bahwasanya PT "A" mendapatkan skor 38 yang artinya level keamanan informasinya masuk ke dalam kategori buruk. Sementara itu, Koperasi "B" mendapatkan skor 52 yang artinya level keamanan informasinya masuk ke dalam kategori kurang. Terakhir, Penerbit "C" mendapatkan skor 54 yang artinya level keamanan informasinya masuk ke dalam kategori kurang. Oleh sebab itu, dapat disimpulkan bahwa level keamanan informasi

untuk ketiganya masih di bawah dari level cukup. Hal itu disebabkan karena fokus ketiganya masih bersifat operasional dan belum berfokus ke arah strategis (seperti keamanan informasi).

Berdasarkan kesimpulan di atas, dapat diberikan saran kepada unit usaha (perusahaan) terkait, yaitu diperlukan peningkatan keamanan informasi dengan menerapkan seluruhnya keamanan yang masih sebagian dan tidak diterapkan. Selain itu, melakukan evaluasi keamanan informasi secara berkala untuk dapat memantau level keamanan informasi. Sementara itu, saran bagi peneliti selanjutnya, yaitu dapat melakukan pengujian efektivitas keamanan yang sudah diterapkan.

Daftar Pustaka

Alshboul, Y., & Streff, K. (2015). Analyzing Information Security Model for Small-Medium Sized Businesses. Twenty-first Americas Conference on Information Systems (pp. 1-9). Puerto Rico: Curran Associates.

Annur, C. M. (2020, Mei 11). *UKM Indonesia Jadi Target 192 Ribu Serangan Siber Selama WFH*. Retrieved from katadata: https://katadata.co.id/happyfajrian/digital/5eb923b47a779/ukm-indonesia-jadi-target-192-ribu-serangan-siber-selama-wfh

Asosiasi Penyelenggara Jasa Internet Indonesia. (2019-2020 (Q2)). *Laporan Survei Internet APJII*. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia.

BSSN. (2020). *Laporan Tahunan Hasil Monitoring Keamanan Siber*. Jakarta: Badan Siber dan Sandi Negara.

BSSN. (2020, Februari). *Penilaian Mandiri Keamanan Informasi (PAMAN KAMI)*. Retrieved from https://bssn.go.id: https://cloud.bssn.go.id/s/2TqsacBESPHky4A#pdfviewer

BSSN. (2020). *Rekap Serangan Siber (Januari - April 2020)*. Jakarta: Badan Siber dan Sandi Negara.

Fauzi, R. (2018). Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002. Jurnal Teknologi Rekayasa, 145-156.

Ozkan, B. Y., Spruit, M., Wondolleck, R., & Coll, V. B. (2020). Modelling adaptive information security for SMEs in a cluster. Journal of Intellectual Capital, 235-256.