SAFEnet

PANDUAN AUDIT KEAMANAN DIGITAL

UNTUK ORGANISASI MASYARAKAT SIPIL

PANDUAN AUDIT KEAMANAN DIGITAL

untuk Organisasi Masyarakat Sipil

SAFEnet
2024

Panduan Audit Keamanan Digital untuk Organisasi Masyarakat Sipil

Oktober 2024

Tim Penyusun [sesuai urutan abjad]
Andreas Takimai
Anton Muhajir
Ardy Wibisana

Pengulas
Andika Triwidada

Ilustrasi & Tata Letak
Crueniaone

Penerbit
Southeast Asia Freedom
of Expression Network (SAFEnet)
Jalan Gita Sura III Nomor 55
Peguyangan Kaja
Denpasar, Bali 80115

+62 811 9223375
info@safenet.or.id
& @safenetvoice
safenet.or.id

Daftar Isi

Pengantar

Teknologi digital sudah menjadi bagian tak terpisahkan dari kerja-kerja organisasi masyarakat sipil. Itu adalah keniscayaan. Teknologi digital telah terbukti membantu dan mempermudah kerja-kerja organisasi masyarakat sipil. Namun demikian, di dalam kemudahan tersebut, terdapat risiko dan ancaman yang berbahaya terhadap organisasi masyarakat sipil itu sendiri maupun terhadap demokrasi dan hak asasi manusia secara lebih luas.

Ketika kita bergantung terhadap perangkat atau alat digital, terdapat tiga komponen keamanan digital yang terkadang luput dari perhatian, yaitu *process* (termasuk kebijakan), *people* (sumber daya manusia), dan *platform* (teknologi yang digunakan). Ketiga hal tersebut saling terkait dan terikat dengan keberlangsungan dan keamanan suatu organisasi. Dari alat yang digunakan pada praktik kerja, perilaku manusia dalam penggunaan teknologi, hingga alat komunikasi sehari-hari, masing-masing memiliki risiko dan ancaman tersendiri.

Salah satu cara memitigasi risiko tersebut adalah dengan melakukan proses evaluasi teknologi yang digunakan, kapasitas sumber daya manusia yang menggunakan, hingga ada tidaknya proses atau kebijakan keamanan digital dan bagaimana penerapannya jika sudah memiliki kebijakan tersebut. Evaluasi ini perlu dilakukan secara rutin, guna menilai kapasitas organisasi dalam menghadapi potensi risiko, ancaman, dan serangan digital yang terus berkembang dan bervariasi.

Selama lima tahun terakhir, SAFEnet telah melakukan pemantauan pelanggaran hak-hak digital, termasuk serangan digital, secara intensif. Hasil pemantauan menunjukan bahwa frekuensi insiden dan

serangan digital terus meningkat selain bentuk dan metode serangan yang juga kian beragam. Berdasarkan pemantauan SAFEnet, pada tahun 2023 terdapat 323 serangan digital dengan latar belakang korban paling banyak berasal dari kelompok kritis, yaitu aktivis, jurnalis, media, dan organisasi masyarakat sipil.

Hal tersebut semakin menekankan urgensi tentang pentingnya keamanan digital bagi organisasi masyarakat sipil sebagai bagian dari kelompok kritis tersebut. Namun, keterbatasan sumber daya menjadi hambatan dalam menerapkan praktik keamanan digital yang optimal. Di sisi lain, kenyamanan pada perilaku lama yang berisiko, sering kali menjadi tantangan dalam menerapkan keamanan digital organisasi secara menyeluruh. Tidak jarang, prinsip "lebih baik mencegah daripada mengobati" jadi terpatahkan karena suatu lembaga, personel, atau organisasi baru sadar bahaya yang mengintai setelah mengalami serangan secara langsung.

Oleh karena itu, kesadaran dan kewaspadaan harus ditingkatkan sebagai upaya preventif menangkal serangan dan insiden digital. Salah satu caranya dengan melakukan pemeriksaan secara keseluruhan aspek yang berkaitan langsung dengan keamanan digital maupun secara tidak langsung.

Sebagai bagian dari upaya meningkatkan kapasitas keamanan digital organisasi masyarakat sipil tersebut, SAFEnet juga melakukan audit keamanan digital bagi organisasi masyarakat sipil sejak tahun 2021. Hingga saat ini, audit telah dilakukan kepada lebih dari 50 organisasi masyarakat sipil yang bekerja di berbagai isu, seperti hukum dan hak asasi manusia, lingkungan, media alternatif, organisasi buruh, serta kelompok minoritas gender dan agama.

Kerangka kerja yang SAFEnet gunakan dalam semua audit keamanan digital tersebut adalah Security Auditing Framework and Evaluation

Template for Advocacy Groups (SAFETAG) yang dikembangkan Internews. Namun, alih-alih menggunakan begitu saja, kami juga melakukan penyesuaian agar lebih sesuai dengan konteks Indonesia. Kami menambahkan juga setidaknya dua hal, yaitu observasi media sosial dan penilaian kapastitas keamanan digital secara mandiri yang kami sebut PAKEM DIRI.

Melihat semakin tingginya kebutuhan audit bagi organisasi masyarakat sipil ini, maka SAFEnet juga terus menambah auditornya. Namun, penambahan auditor saja tidak cukup. Perlu ada juga auditor-auditor keamanan digital lain dengan tetap mengacu pada panduan yang sudah diterapkan SAFEnet.

Dengan tujuan agar semakin banyak staf organisasi masyarakat sipil bisa mengaudit keamanan digital lembaganya sendiri, maka SAFEnet juga melaksanakan pelatihan audit keamanan digital pada Mei 2024 di Bandung. Panduan ini dibuat sebagai bagian tak terpisahkan dari pelatihan yang diadakan dalam program Greater Internet Freedom (GIF) Internews dengan mitra regional EngageMedia dan SAFEnet sebagai mitra lokal. Dalam pelatihan dua hari tersebut, para peserta juga membahas sekilas bagian-bagian dalam panduan ini.

Panduan ini tetap menggunakan SAFETAG sebagai referensi utama, terutama dari sisi konten dan struktur pelaksanaannya. Namun, sekali lagi, kami juga mengadaptasi pengalaman sendiri selama melakukan audit empat tahun terakhir di Indonesia. Kami juga melengkapinya dengan reviu oleh ahli keamanan digital dan diskusi kelompok terfokus yang diikuti staf teknologi informasi organisasi yang sudah berkolaborasi dengan SAFEnet selama ini dalam upaya meningkatkan kapasitas keamanan digital bagi organisasi masyarakat sipil di Indonesia.

Dengan demikian, kami berharap pengalaman tersebut akan mem-

perkaya materi panduan sekaligus menjadikannya agar lebih relevan.

Terima kasih untuk semua pihak yang sudah berjibaku menyusun ulang materi ini, terutama tim penyusun, pengulas, dan peserta pelatihan maupun diskusi terfokus. Kami yakin semua proses tersebut akan menjadi modal penting dalam meningkatkan kapasitas keamanan digital masyarakat sipil Indonesia di tengah semakin kuatnya represi digital saat ini.

Denpasar, September 2024

SAFEnet

Tentang Panduan

Panduan ini merupakan referensi untuk melaksanakan audit keamanan digital bagi organisasi masyarakat sipil menggunakan kerangka kerja (*framework*) SAFETAG. Materi dalam panduan ini sebagian besar diterjemahkan dari materi panduan SAFETAG dengan penyesuaian untuk konteks Indonesia, terutama untuk organisasi masyarakat sipil.

Kami menambahkan pengalaman SAFEnet yang selama empat tahun terakhir juga melakukan audit keamanan digital menggunakan metode SAFETAG untuk organisasi masyarakat sipil di Indonesia. Audit tersebut dilakukan untuk berbagai organisasi, dalam bentuk perkumpulan, yayasan, kolektif, atau sekadar kelompok dukungan sebaya. Fokus kegiatan mereka juga beragam, seperti lingkungan, demokrasi dan hak asasi manusia, masyarakat adat, perempuan, serta lesbian, gay, biseksual, transgender, dan queer (LGBTQ).

Pengalaman melakukan audit kepada lebih dari 50 organisasi masyarakat sipil selama empat tahun terakhir tersebut menjadi modal penting dalam penyusunan panduan ini.

Sasaran pengguna panduan ini adalah staf yang sudah memiliki pengetahuan dan keterampilan dasar keamanan digital, khususnya terkait organisasi masyarakat sipil. Hal ini penting karena beberapa pengetahuan dan keterampilan dasar diperlukan untuk dapat menggunakan panduan ini dalam melakukan audit.

Meskipun demikian, pengetahuan dan keterampilan dasar tersebut juga bukan hal paling penting dalam pelaksanaan audit, karena masalah teknis hanya menjadi salah satu bagian dari keseluruhan proses audit. Proses audit menggabungkan setidaknya tiga aspek,

yaitu analisis risiko dan ancaman, kapasitas organisasi, dan perilaku staf.

Panduan ini juga sekadar acuan umum dalam pelaksanaan audit keamanan digital. Penerapannya sangat fleksibel dan bisa disesuaikan dengan kapasitas organisasi yang diaudit serta kebutuhan mereka. Tahapannya bisa dibuat lebih ringkas, begitu pula dengan komponen-komponen yang harus diaudit selama tujuan akhirnya untuk menemukan risiko dan ancaman pun memberikan rekomendasi untuk meningkatkan keamanan digital bisa tercapai.

Tentang SAFETAG

SAFETAG adalah kerangka kerja dan templat untuk melakukan audit keamanan bagi organisasi masyarakat sipil. Kerangka kerja ini mengadopsi teknis uji penetrasi (*penetration testing*) dan metodologi pemodelan ancaman (*threat modelling*) yang disesuaikan agar relevan dengan organisasi nirlaba yang lebih kecil.

SAFETAG bukan pelatihan maupun penerapan kontrol keamanan. SAFETAG tidak mendefinisikan hanya satu set kegiatan untuk segala macam organisasi dengan isu yang beragam, tetapi perlu dipilih kegiatan mana yang cocok. SAFETAG juga bukan kerangka untuk memberikan respon insiden secara cepat (*rapid response*).

SAFETAG sebagai suatu kerangka kerja dapat dipakai sebagai suatu acuan yang fleksibel dan dapat diadaptasi ke satu masalah yang spesifik. Apa yang bisa kita ambil dari kerangka kerja SAFETAG bergantung kepada konteks, keahlian auditor, sumber daya (waktu, finansial, kapasitas), dan cakupan serta kebutuhan spesifik. Sehingga, proses audit keamanan digital tidak perlu berjalan secara kaku yang berdasarkan standar-standar kompleks yang digunakan oleh industri teknologi besar. Lebih dari itu juga bahwa audit keamanan memerlukan uang, waktu, dan kapasitas yang tidak bisa dibilang kecil.

SAFETAG tidak dirancang untuk memberi skor terhadap tingkat risiko keamanan digital suatu organisasi. SAFETAG berfokus pada mendeteksi kesenjangan dalam strategi keamanan organisasi untuk merekomendasikan tindak lanjut yang spesifik dan relevan.

Berdasarkan temuan laporan evaluasi dampak audit SAFETAG oleh Purpose+Motion dan Internews, pemakaian kerangka kerja SAFETAG telah meningkatkan keamanan digital bagi berbagai organisasi, ter-

masuk peningkatan kesadaran akan risiko-risiko, perilaku keamanan, dan penerapan rekomendasi yang diberikan. Bukti tersebut menunjukkan tingginya relevansi dan potensi pemanfaatan kerangka kerja ini untuk menilai dan meningkatkan kapasitas organisasi. Maka dari itu, SAFEnet sebagai organisasi yang telah juga merasakan manfaat atas kerangka ini dalam berbagai kegiatannya, menerbitkan panduan ini sebagai upaya untuk meningkatkan kapasitas organisasi masyarakat sipil di Indonesia.

MATERI DAN STRUKTUR

SAFETAG terdiri dari kumpulan metodologi yang mencakup hal umum, setiap metode juga terkait dengan kegiatan-kegiatan yang dapat dilakukan untuk mencapai tujuan audit, yaitu setidaknya analisis risiko dan ancaman, kapasitas organisasi, dan perilaku staf. Dalam melaksanakan Kegiatan yang diperlukan, terdapat tiga pendekatan yang dapat dilalui: Teknis, Riset, dan Interpersonal.

Pemilihan pendekatan sangat condong dengan gaya atau keahlian dari setiap auditor itu sendiri. Misalnya, seseorang yang memiliki latar belakang dari pelatihan keamanan digital biasanya condong melakukan pendekatan interpersonal, lalu, seseorang dengan latar belakang keamanan siber dengan pendekatan teknis. Kendati demikian, dengan menggunakan kombinasi dari setiap pendekatan yang ada, auditor akan lebih mendapatkan gambaran dan pemahaman lebih mendalam tentang bagaimana organisasi bekerja. Selain hanya informasi tentang infrastuktur digital organisasi, tetapi dapat menggali juga informasi bagaimana pengambilan keputusan dilakukan, bagaimana kebijakan diterapkan atau tidak, dan bagaimana potensi perubahan yang dapat organisasi tempuh.

Setiap auditor, khususnya yang berpengalaman, akan sangat mungkin memilih proses pendekatannya sendiri. Struktur dari SAFETAG pun tersusun atas 18 metode dan 73 kegiatan. Isi metode cukup umum,

mencakup aspek-aspek luas terkait keamanan organisasi. Tidak selalu berhubungan dengan aspek-aspek digital. Setiap metode diuraikan lagi ke kegiatan. Ada beberapa kegiatan yang sama terkait ke beberapa metode berbeda. Oleh karena itu, penyesesuaian dengan konteks lokal di Indonesia kami sesuaikan dan rancang menjadi tahapan atau bagian yang terdapat dalam panduan ini.

Bagaimana SAFETAG Disusun

Metode

Tinjauan Kebijakan Organisasi

Metodologi ini mengeksplorasi praktik-praktik organisasi yang ada, perjanjian informal, dan kebijakan seputar pengelolaan keamanan informasi dan menanggapi ancaman. Metodologi ini juga berusaha untuk mengungkapkan asumsi yang dibuat ...

Kegiatan

Mengidentifikasi Perjanjian Informal

Kegiatan ini bertujuan untuk menilai jenis perjanjian informal mengenai praktik terbaik dan arahan keamanan yang dirumuskan, diakses, ...

Tinjauan Kebijakan Kemanan

Kegiatan ini bertujuan untuk memahami konteks kebijakan keaman internal organisasi, mencari kebijakna yang ada, memahami bagaimana kebijakan tersebut ...

Wawancara

Auditor melakukan wawancara dengan berbagai anggota staf untuk mengumpulkan informasi tentang risiko dan kapasitas organisasi. Sesi tanya jawab adalah ...

Materi 1:
Persiapan dan Perencanaan

RINGKASAN

Sebelum melaksanakan audit, auditor terlebih dahulu harus membuat persiapan dan perencanaan. Tujuan tahapan ini untuk membuat perjanjian kerja sama dan perjanjian kerahasiaan atau *non-disclosure agreement* (NDA) dengan organisasi yang diaudit, khususnya jika auditor adalah pihak eksternal. Persiapan ini juga termasuk menentukan ruang lingkup, tahapan, dan jadwal audit. Materi persiapan juga termasuk daftar pertanyaan audit dan dokumen PAKEM DIRI.

Rangkaian audit tersusun atas tahap persiapan, pelaksanaan, dan penyusunan laporan. Beberapa audit mungkin memiliki tahapan ekstra, yaitu tahap perbaikan dan tahap uji ulang. Pendekatan yang mencakup dua tahap tambahan ini lebih komprehensif dan memuaskan karena diharapkan setelah rangkaian kegiatan audit selesai, sudah tidak ada lagi (atau sangat minim) sisa masalah yang ditemui saat audit.

Perlu menjadi catatan juga bahwa keterlibat tim manajemen dalam proses audit sangat krusial dan penting untuk keberhasilan audit. Menurut hasil laporan evaluasi SAFETAG oleh Purpose+motion, 95% auditor dan organisasi yang diaudit merasakan bahwa partisipasi manajemen merupakan suatu hal yang penting dalam keberhasilan proses audit. Hal ini senada dengan pengalaman-pengalaman SAFEnet.

TAHAPAN

Kegiatan yang harus dilakukan dalam tahap persiapan termasuk:

- Pembuatan perjanjian kerahasiaan dan perjanjian kerja sama
- Pengumpulan informasi organisasi dari jarak jauh
- Prosedur penanganan insiden
- Interview pra audit
- Penyusunan tahapan dan jadwal dan pemilihan kegiatan
- Pembahasan PAKEM DIRI
- Persiapan auditor

Pembuatan Perjanjian

Perjanjian Kerja Sama dan Perjanjian Kerahasiaan (*Non-Disclosure Agreement*) ini diperlukan sebagai jaminan tertulis atau bahkan dasar hukum bahwa kedua belah pihak, yaitu auditor dan organisasi yang diaudit, sepakat melakukan kerja sama audit dan akan menjaga kerahasiaan satu sama lain. Hal ini karena selama proses audit akan banyak informasi internal organisasi yang diaudit akan dibagikan ke auditor untuk diperiksa atau diungkap sebagai bahan diskusi dan kegiatan audit lain, termasuk data dan informasi yang bersifat rahasia dan konfidensial.

Kedua dokumen tersebut bisa jadi terpisah, misalnya bila diperlukan untuk membuat NDA bagi masing-masing personel audit yang terlibat, bukan hanya satu atas nama organisasi pelaksana audit. Perjanjian kerja sama cukup satu untuk masing-masing pihak.

Perjanjian Kerja Sama ini setidaknya harus mencantumkan informasi berikut:

- **Identitas** kedua belah pihak yaitu nama auditor dan organisasi, alamat, dan kontak masing-masing.
- **Tujuan audit** yaitu untuk apa audit tersebut dilakukan.

- **Ruang lingkup** yaitu apa saja yang akan diaudit, seperti profil organisasi, risiko dan ancaman, kapasitas organisasi, kebijakan keamanan digital (jika ada), dan aset-aset digital organisasi.
- **Periode** yaitu berapa lama audit akan dilaksanakan dan dari tanggal berapa hingga tanggal berapa.
- **Hak dan kewajiban** masing-masing pihak baik auditor dan organisasi yang diaudit, misalnya, kewajiban bagi organisasi untuk memberikan informasi yang diperlukan dan kewajiban auditor untuk bekerja secara profesional.
- **Kerahasiaan data** yaitu jaminan bahwa auditor tidak akan membocorkan data dan informasi organisasi kepada pihak lain.
- **Informasi tambahan** termasuk kemungkinan perubahan periode kerja jika audit tidak selesai selama periode yang sudah disepakati.

Perjanjian Kerahasiaan ini setidaknya harus mencantumkan informasi berikut:

- **Identitas** kedua belah pihak yaitu nama auditor dan organisasi, alamat, dan kontak masing-masing.
- **Hak dan kewajiban** masing-masing pihak baik auditor dan organisasi yang diaudit, misalnya, kewajiban bagi organisasi untuk memberikan informasi yang diperlukan dan kewajiban auditor untuk bekerja secara profesional.
- **Kerahasiaan data** yaitu jaminan bahwa auditor tidak akan membocorkan data dan informasi organisasi kepada pihak lain.
- **Penyelesaian Sengketa** merupakan bagian dalam Perjanjian Kerahasiaan untuk membantu memastikan kerahasiaan data tetap terjaga apabila terjadi perselisihan atau perbedaan pendapat antara kedua belah pihak.

Pengumpulan Informasi Jarak Jauh

Dalam tahap ini, auditor mengumpulkan berbagai informasi umum terkait organisasi, sebagai bahan awal untuk menggali lebih dalam organisasi yang akan diaudit. Berbagai hal yang ditemukan saat pencarian informasi ini dapat mengarah ke usulan kegiatan yang relevan.

Informasi yang dikumpulkan dapat berupa situs-situs web, extranet, server email, serta juga informasi media sosial. Umumnya, informasi tersebut tersedia secara publik, sehingga proses pengumpulan bisa dilakukan secara mandiri.

Prosedur Penanganan Insiden

Tindakan penangan insiden seharusnya dilakukan sesuai dengan kebijakan dan prosedur yang berlaku dalam organisasi yang diaudit. Namun, tidak semua organisasi telah memiliki kebijakan terkait. Oleh sebab itu, auditor perlu memerhatikan langkah yang perlu dilakukan jika ia menemukan atau menyebabkan suatu insiden ketika melakukan asesmen dalam tahap manapun dalam rangkaian audit.

Tidak ada prosedur pasti dalam menangani insiden, tetapi beberapa hal yang dapat dilakukan supaya meminimalisir dampak buruk adalah:

- **Pengendalian (*Containment*)**

  Pengendalian atau Containment adalah langkah pertama yang harus dilakukan jika ditemukan suatu insiden keamanan dalam audit. Tujuannya untuk menghentikan atau mengendalikan dampak negatif dari insiden tersebut secepat mungkin. Dalam containment, auditor harus:

  - Mencari sumber insiden dan mematikan atau menonaktifkannya.
  - Mengecek semua sistem dan aplikasi terkait untuk memastikan tidak ada efek samping lainnya.

- **Pemulihan (*Recovery*)**
  - Memulihkan sistem agar kembali berfungsi normal.
- **Dokumentasi (*Documentation*)**
  Setelah insiden dikendalikan, langkah berikutnya adalah merekam dan mendokumentasikan semua detail mengenai kejadian tersebut. Hal ini penting untuk:
  - Mengenali penyebab insiden dan menghindari dampak yang serupa di masa depan.
  - Mengetahui tingkat kerusakan dan apa yang harus dilakukan untuk memulihkan sistem atau aplikasi yang terdampak.
- **Pelaporan (Reporting)**
  - Penanganan insiden tidak berhenti pada tahap dokumentasi. Namun, Auditor harus melaporkan kejadian tersebut terhadap pihak-pihak yang terlibat.

Interview Sebelum Audit

Materi lain yang perlu disiapkan dalam tahap persiapan dan perencanaan adalah penyiapan dokumen PAKEM DIRI. PAKEM DIRI merupakan penilaian keamanan digital secara mandiri (*self assessment*) yang dikembangkan SAFEnet berdasarkan perilaku individu terkait keamanan digital.

Ada 50 pertanyaan dalam PAKEM DIRI yang terbagi dalam empat kategori keamanan digital, yaitu kebersihan perangkat, manajemen identitas, keamanan komunikasi, dan keamanan ponsel. Informasi lebih detail mengenai PAKEM DIRI bisa diakses di tautan https://pakemdiri.safenet.or.id.

Sebagai bagian dari persiapan audit, auditor perlu menjelaskan kepada organisasi yang diaudit tentang metode PAKEM DIRI, apa tujuannya, bagaimana cara mengisi, dan kapan harus menyerahkan semua hasilnya. Perlu ditekankan bahwa meskipun PAKEM DIRI

bersifat individual, tetapi hasil rata-rata akan memerlihatkan sejauh mana organisasi telah menerapkan keamanan digital dan apa saja praktik keamanan yang belum diterapkan sehingga memengaruhi risiko keamanan digital organisasi.

Penyusunan Tahapan dan Jadwal

Setelah ada perjanjian kerja sama dan perjanjian kerahasiaan dan langkah persiapan lain di atas, auditor harus menyiapkan tahapan dan jadwal pelaksanaan audit. Kesepakatan tahapan dan jadwal ini berguna sebagai acuan bagi kedua belah pihak terutama dalam persiapan waktu dan apa saja dokumen yang perlu disiapkan organisasi yang akan diaudit.

Perlu didefinisikan juga usulan aktivitas SAFETAG apa saja yang relevan dalam proses audit.

Contoh tahapan dan dokumen tersebut bisa dilihat dalam tabel berikut:

Tahapan	Kebutuhan
Perencanaan dan Persiapan	Perjanjian kerahasiaan, alur kerja dan formulir penilaian yang disepakati kedua belah pihak
Penilaian Keamanan Perangkat	Formulir penilaian, jadwal wawancara staf
Penilaian Keamanan Website	Daftar website mitra dampingan
Penilaian Keamanan Jaringan	Admin jaringan
Pemetaan Risiko dan Mitigasi	Form penilaian
Penilaian Kebijakan Keamanan	Penemuan kerentanan dan rencana aksi
Penyusunan SOP Keamanan Digital	Kebijakan dan SOP Keamanan Digital untuk organisasi

Penyusunan Laporan Akhir	Laporan audit, pemindaian, dan hasil wawancara & SOP Keamanan Digital

Persiapan Auditor

Auditor perlu juga secara mandiri melakukan persiapan audit, mencakup beberapa hal:

- Memastikan peralatan bantu audit sudah tersedia dan siap dipakai (*hardware, software, checklist*, alat bantu lain)
- Rencana perjalanan, akomodasi, transportasi, dan logistik lain yang diperlukan pada saat audit.

Pada kondisi tertentu ketika melakukan audit terhadap organisasi dengan risiko tingkat tinggi, perlu juga persiapan manajemen risiko yang baik.

TINDAK LANJUT

Keluaran (output) yang diharapkan

- Perjanjian dengan organisasi yang akan diaudit, mencakup lingkup, linimasa, kebijakan konfidensialitias/NDA, dan nomor kontak.

ACUAN

Activities SAFETAG terkait:

- Assessment Plan
  https://safetag.org/activities/assessment_plan
- Confidentiality Agreement
  https://safetag.org/activities/confidentiality_agreement
- Incident Response and Emergency Contact
  https://safetag.org/activities/incident_response
- Regional Context Research
  https://safetag.org/activities/regional_context_research

- Technical Context Research
  https://safetag.org/activities/technical_context_research
- Audit Timeline and Planning
  https://safetag.org/activities/safetag_audit_timeline
- Incident Response
  https://safetag.org/activities/incident_response/

Materi 2:
Penilaian Risiko dan Ancaman

RINGKASAN

Pada dasarnya, SAFETAG adalah kerangka penilaian risiko keamanan informasi pada sebuah organisasi. Penilaian risiko diartikan sebagai pendekatan sistematis untuk mengidentifikasi dan menilai risiko terkait potensi bahaya terhadap aktivitas manusia yang terorganisir. SAFETAG memfokuskan pendekatan pada risiko keamanan informasi. Audit SAFETAG berupaya mengumpulkan jenis informasi berikut untuk menilai risiko yang dihadapi organisasi.

Risiko adalah penilaian terhadap kemungkinan terjadinya peristiwa berbahaya. Risiko dinilai dengan membandingkan ancaman yang dihadapi suatu organisasi dengan kerentanannya dan kapasitasnya untuk merespons atau memitigasi ancaman yang muncul.

SAFETAG berkisar pada pengumpulan informasi yang cukup untuk mengidentifikasi dan menilai berbagai risiko yang dihadapi suatu organisasi dan aktor terkait sehingga mereka dapat mengambil tindakan secara strategis.

TAHAPAN

Secara umum pendekatan audit berbasis risiko dimulai dengan identifikasi risiko, analisis tingkat risiko, penentuan prioritas penanganan risiko, dan alternatif penanganan/mitigasi risiko. Pendekatan ini mengakomodasi kenyataan bahwa tidak semua risiko yang ada dapat ditangani karena berbagai keterbatasan: sumber daya manusia, waktu, finansial, tingkat kesulitan teknis, dsb. Dengan diiden-

tifikasinya berbagai risiko dan tingkat keparahan atau *severity*-nya, digabung dengan tingkat kemungkinan terjadinya, yang menghasilkan tingkat dampak, maka organisasi dapat menentukan prioritas agar peningkatan keamanan organisasi dapat dilaksanakan dengan cara yang paling efektif dan efisien.

SAFETAG membagi analisis risiko menjadi tiga bagian, yaitu Analisis Program, Analisis Kerentanan, dan Analisis Ancaman.

Analisis Program

Tahap ini merupakan waktu tepat untuk menggali lebih dalam bagaimana alur dari kegiatan atau program yang organisasi jalani. Mengenali cara kerja, proses, atau alur dapat membantu alur menganalisis bagaimana organisasi bekerja.

Analisis program dilakukan untuk mengidentifikasi tujuan utama organisasi dan menentukan kapasitasnya. Proses ini memaparkan aktivitas, aktor, dan kapasitas suatu organisasi. Contohnya apa saja kegiatan yang dilakukan organisasi untuk mencapai tujuannya.

Aktivitas

Kegiatan yang dilakukan organisasi untuk mencapai tujuannya. Misalnya, kampanye, penggalangan dana, advokasi

Kegiatan adalah tindakan dan proses organisasi. Meskipun sebagian besar pekerjaan NGO berkisar pada konsep berbasis program, kegiatan-kegiatannya juga mencakup hal-hal yang berhubungan dengan keamanan digital. Misalnya dengan menilai Kegiatan organisasi mencakup kebijakan dan prosedur yang diterapkan untuk melindungi informasi. Ini termasuk pengembangan kebijakan keamanan, pelatihan staf, manajemen risiko, serta monitoring dan tanggapan terhadap insiden.

Dalam analisis program, penting untuk mengevaluasi seberapa efektif aktivitas-aktivitas ini dalam menciptakan lingkungan yang aman. Misalnya, apakah kebijakan keamanan diperbarui secara berkala dan diterapkan dengan konsisten? Apakah staf mendapatkan pelatihan yang memadai untuk mengenali dan merespons ancaman? Dengan menganalisis aktivitas ini, organisasi dapat mengidentifikasi area yang perlu diperbaiki dan memastikan bahwa langkah-langkah yang diambil relevan dengan risiko yang dihadapi.

Aktor

Aktor adalah orang-orang yang terhubung dengan suatu organisasi, termasuk staf, dewan pengurus/pengawas, dan mitra organisasi. Aktor juga dapat mencakup sukarelawan, jaringan, penerima manfaat, dan donor.

Selain itu, aktor dalam organisasi, termasuk staf IT, manajemen, anggota dewan, dan pengguna akhir, memainkan peran penting dalam implementasi dan keberhasilan program keamanan. Analisis program harus mencakup penilaian terhadap peran dan tanggung jawab masing-masing aktor. Ini melibatkan pemahaman tentang sejauh mana setiap aktor dilibatkan dalam kebijakan keamanan dan seberapa efektif mereka berkolaborasi untuk mencapai tujuan bersama.

Ketidakjelasan dalam peran atau kurangnya pelatihan bagi pengguna dapat menciptakan celah keamanan yang signifikan. Dengan menilai interaksi antaraktor, organisasi dapat memperkuat kolaborasi dan memastikan bahwa semua pihak memahami peran mereka dalam menjaga keamanan.

Kapasitas

Indikator kapasitas yang mencakup keterampilan staf dan berbagai

macam sumber daya yang dapat dimanfaatkan organisasi untuk memengaruhi perubahan termasuk pendanaan, jaringan, serta proses dan kebijakan kelembagaan.

Kapasitas organisasi mencakup sumber daya dan kemampuan yang tersedia untuk mendukung program keamanan digital. Ini meliputi keterampilan staf, infrastruktur keamanan, kebijakan yang ada, serta pendanaan yang dialokasikan untuk inisiatif keamanan.

Dalam analisis program, penting juga untuk mengevaluasi apakah kapasitas ini mencukupi untuk menghadapi ancaman yang dapat muncul. Apakah staf memiliki keterampilan dan pengetahuan yang diperlukan untuk menjalankan penerapan keamanan yang efektif? Apakah teknologi yang digunakan memadai dan terus diperbarui? Dengan melakukan penilaian ini, organisasi dapat mengidentifikasi kelemahan dalam kapasitas yang mungkin membatasi efektivitas program keamanan dan menentukan area yang memerlukan investasi lebih lanjut.

Analisis Kerentanan

Analisis kerentanan dilakukan untuk mengetahui paparan ancaman, titik lemah, dan cara-cara lain untuk memengaruhi organisasi. Contohnya isu yang dikerjakan, praktik mitigasi yang belum dilakukan, dan sejauh mana ketergantungannya pada teknologi digital. Langkah ini serupa dengan seseorang yang melakukan *medical check up* untuk memeriksa apakah seseorang menderita penyakit tertentu dan seberapa parah. Langkah ini sangat penting karena berbeda dengan analisis program dimana organisasi yang diaudit sangat familiar dengan berbagai aspeknya, maka analisis kerentanan ini berusaha mengidentifikasi masalah dan potensi masalah yang belum tentu disadari keberadaannya oleh organisasi, sehingga sangat boleh jadi perlu auditor dari luar untuk memeriksanya.

Selama pengalaman SAFEnet melakukan audit keamanan digital dan melakukan pemantauan pelanggaran hak-hak digital, khususnya terkait insiden atau serangan digital. Beberapa temuan yang sering ditemui adalah hal-hal seperti pengambilalihan akun, penggunaan credentials bawaan (*default*), dan kehilangan data.

Analisis Ancaman

Adapun analisis ancaman adalah proses mengidentifikasi penyerang potensial dan mengumpulkan informasi latar belakang tentang kemampuan penyerang tersebut untuk mengancam organisasi. Dasar dari informasi ini adalah riwayat ancaman yang pernah terjadi terhadap organisasi.

Utamanya, organisasi tidak akan luput dari ancaman digital secara umum. Kendati demikian, organisasi masyarakat sipil, khususnya yang bergerak dengan isu sensitif, rentan mengalami dan menjadi target lebih intens.

Dalam konteks OMS, tiap organisasi yang bergerak di isu tertentu memiliki kecondongan ancaman yang dialami.

Latar Belakang	Serangan halus (non-teknis)	Serangan Kasar (teknis)	Keterangan
Papua	• Trolling • Sextortion • Impersonasi • Intimidasi	• DDoS Attack • Pemutusan kabel Internet • Robocall • Zoom Bombing • Pencurian laptop	
Lingkungan	• Doxing • Intimidasi	• Peretasan situs web • Pengambilalihan akun	

LGBTQ	• NCII • Impersonasi Online • exhibitionism Trolling	• Peretasan akun media sosial • Peretasan akun pesan ringkas	Terkait erat dengan KBGO
Jurnalis	• Doxing • Trolling	• DDoS Attack • Peretasan Akun	
Demokrasi dan HAM		Pengambilalihan Instagram dan WhatsApp	
Perem-puan	Impersonasi		Relatif lebih rendah risikonya

Sumber: Sudah Rentan, Kurang Waspada Pula. 2022.

Berikut adalah contoh pertanyaan yang perlu dijawab untuk mengetahui sejauh mana risiko dan ancaman organisasi:

- Profil dan Struktur Organisasi
  - Bagaimana profil organisasi?
  - Bagaimana struktur organisasi?
  - Apa tugas dan fungsi masing-masing dalam struktur tersebut?
- Program dan Kegiatan
  - Apa saja program dan kegiatannya?
  - Siapa sasaran utama program organisasi?
  - Apa saja kegiatan dan isu penerima manfaat programnya?
- Penggunaan Teknologi
  - Bagaimana penggunaan teknologi digital oleh organisasi?
  - Sejauh mana mereka tergantung pada teknologi tersebut?
- Risiko dan Ancaman Digital

- Apa saja risiko dan ancaman serangan digital yang mungkin terjadi?
- Seberapa besar kemungkinan dan intensitasnya?
- Apa saja riwayat serangan yang pernah terjadi?
- Jika pernah terjadi, bagaimana dampaknya? Bagaimana penanganannya?

- Pelaku Ancaman dan Teknik Serangan
  - Apakah bisa diketahui siapa pelaku ancaman dan serangan tersebut?
  - Teknik apa yang mereka gunakan?
  - Apakah mereka menargetkan kerentanan organisasi saat ini?
  - Apakah mereka menargetkan organisasi serupa atau hanya menyasar organisasi yang diaudit?
  - Apa saja metode yang digunakan oleh pelaku ancaman untuk menyerang organisasi serupa?
  - Apakah pelaku ancaman saat ini mempunyai keinginan untuk melakukan serangan terhadap organisasi jenis ini?
  - Apakah organisasi merupakan target ancaman prioritas bagi pelaku ancaman?

Semua proses tanya jawab tersebut bisa dilakukan melalui wawancara secara tatap muka maupun secara daring. Namun, metode yang paling baik adalah melalui diskusi terfokus secara langsung bersama semua staf organisasi.

TINDAK LANJUT

Hasil dari penilaian dan analisis risiko dapat menghasilkan peta risiko dan ancaman organisasi. Setiap risiko dan ancaman perlu disesuaikan dengan tingkat atau dampak kerentanan. Untuk mempresentasikan informasi ini, salah satu metode yang dapat digunakan adalah menggunakan tabel dan juga matriks risiko, sebagaimana contoh berikut.

Kegiatan	Risiko dan Ancaman
Pengelolaan dan kampanye media sosial	• Peretasan • Pengambilalihan akun • Phishing • Persekusi daring
Aktivitas daring pada kantor	• Penyadapan • Pengawasan ilegal
Komunikasi Internal	• Peretasan • Penyadapan • Pengambilalihan akun

Kemungkinan Rendah, Dampak Tinggi • Penyadapan • Pengawasan ilegal • Kebocoran data • Serangan Malware • Ransomware	**Kemungkinan Tinggi, Dampak Tinggi** • Peretasan • Pengambilalihan akun • Serangan DDOS • Persekusi daring • Pengancaman • Phising
Kemungkinan Rendah, Dampak Rendah • Injeksi Iklan • Komentar Spam	**Kemungkinan Tinggi, Dampak Tinggi** • Malvertising

Masalah yang teridentifikasi dalam tahap ini dapat ditangani dengan berbagai cara. Aspek pertama, adalah bahwa penanganan perlu dilakukan dengan perbaikan pada satu atau lebih dari SDM, proses (kebijakan dan atau prosedur), dan platform (perangkat keras, perangkat lunak).

Aspek kedua adalah bahwa risiko dapat ditangani dengan cara:

- *Avoid:* menghindari risiko (sepenuhnya mengeliminasi risiko)

- *Mitigate:* memitigasi risiko (mengurangi kemungkinan terjadi atau dampak terjadinya risiko)
- *Transfer:* memindahkan risiko (memindahkan risiko ke pihak ke tiga misanya dengan mengasuransikan)
- *Accept:* menerima risiko (mengonfirmasi keberadaan risiko tetapi tidak melakukan tindakan avoid, mitigate, maupun transfer)

Idealnya kita ingin agar semua risiko dapat dieliminasi sepenuhnya (avoid), tetapi kenyataannya, hal itu tidak mungkin. Maka perlu dipilih risiko mana penanganan terbaiknya dengan cara apa. Misi dan tujuan organisasi bisa dijadikan aspek pertimbangan untuk pemilihan salah satu opsi mitigasi risiko mana yang sebaiknya dipilih. Hal tersebut juga perlu menekankan pertimbangan terhadap skala prioritas, penilaian, ancaman, atau kerentanan yang berpotensi berdampak atau membahayakan secara signifikan.

Keluaran yang diharapkan

Berdasarkan penilaian ini hasil yang akan didapatkan adalah sebagai berikut:

- Data pemetaan risiko pada jaringan dan perangkat organisasi yang diaudit.
- Daftar pemetaan risiko dari program dan kegiatan inti organisasi.
- Daftar pengidentifikasian pemetaan risiko dalam bentuk tabel dan matriks.

ACUAN

Methods SAFETAG terkait:

- Process Mapping and Risk Modeling
  https://safetag.org/methods/risk_modeling
- Threat Assessment
  https://safetag.org/methods/threat_assessment

Activities SAFETAG terkait:

- Process Mapping
  https://safetag.org/activities/process_mapping_activity/
- Risk Modeling Using the Pre-Mortem Strategy
  https://safetag.org/activities/pre_mortum_risk_assessment_activity/
- Creating a Risk Matrix
  https://safetag.org/activities/risk_matrix/
- Sensitive Data
  https://safetag.org/activities/sensitive_data/
- Self Doxing
  https://safetag.org/activities/self_doxing/
- Guiding Questions for High-Risk Organisations
  https://safetag.org/activities/interviews_highrisk/
- Threat Identification
  https://safetag.org/activities/threat_identification/
- Threat Interaction
  https://safetag.org/activities/threat_interaction/
- Regional Context Research
  https://safetag.org/activities/regional_context_research/
- Assessing Legal Threats
  https://safetag.org/activities/assessing-legal-threats/

Materi 3:
Penilaian Data

RINGKASAN

Suatu organisasi mempunyai berbagai macam data. Di sektor atau isu apapun bekerja, setiap organisasi sangat mungkin untuk mengelola data sensitif atau data pribadi. Namun, berkas atau fail sensitif tersebut terkadang tersimpan dalam berbagai perangkat dengan tingkat keamanan berbeda-beda. Tidak menutup kemungkinan, data tersebut kemudian tercecer tanpa disadari. Untuk itu, penting untuk melakukan pengelompokan data, di mana data terkait tersimpan, bagaimana disimpannya, pengamanannya seperti apa, dibagikan kepada siapa dan untuk apa, serta siapa saja yang bisa mengakses. Hal-hal tersebut harus terorganisir dengan baik.

Selain perihal penyimpananan, auditor juga perlu mencari informasi tanggung jawab dan konsekuensi atas bagaimana organisasi menangani data tersebut. Kemungkinan akan kebocoran atau penyalahgunaan data harus dipertimbangkan terhadap organisasi yang mengumpulkan, memproses, dan menggunakan data.

Secara umum, keamanan sistem informasi yang salah satu komponen pentingnya adalah keamanan data, mencakup tiga syarat yang biasa disingkat CIA, meliputi c*onfidentiality* (kerahasiaan), *integrity* (keutuhan), dan *availability* (ketersediaan). Masing-masing syarat akan dijelaskan lebih lanjut di bawah.

Kemanan Data

Kerahasiaan

Beberapa macam data harus dijaga kerahasiaannya, misalnya, kredensial yang dipakai untuk mengakses akun e-mail atau untuk

mengedit konten web (CMS). Ada juga data yang sama sekali tidak perlu dirahasiakan, misalnya, seluruh konten web organisasi yang memang disajikan untuk pengunjung web. Apabila ada konten web yang ingin dibatasi aksesnya (dirahasiakan dari publik, tapi diizinkan diakses oleh pengguna tertentu), maka biasanya disediakan mekanisme akses tertentu, misalnya dengan memakai kredensial (*username & password*).

Kerahasiaan data seringkali memiliki batasan waktu. Suatu dokumen laporan mungkin harus dirahasiakan selama sekian waktu, setelah rentang waktu tersebut, tidak perlu dirahasiakan lagi.

Kata kunci utama terkait kerahasiaan data ini adalah enkripsi. Dengan memakai enkripsi, maka ketika data jatuh ke tangan pihak lain yang mestinya tidak berhak mengaksesnya, mereka tidak akan dapat melihat/membaca data tersebut. Langkah pertama melindungi data adalah upaya agar orang yang tidak berhak tidak bisa mengaksesnya, terutama akses fisik. Setelahnya, pembatasan akses logik.

Kebiasaan *sharing* akun sangat berpengaruh ke perlindungan kerahasiaan. Masalah yang bisa timbul adalah, ketika terjadi insiden kebocoran data, siapa dari para pemegang akun bersama itu yang benar-benar mengakses dan atau menyebabkan kerahasiaan data terbongkar.

Keutuhan

Keutuhan data adalah karakteristik yang sangat penting. Data pada berbagai proses organisasi memang bisa berubah, tetapi perubahannya perlu dijamin memang merupakan perubahan yang diinginkan, dilakukan oleh pihak yang memang memiliki hak, dan dilindungi sehingga mudah terdeteksi apabila ada perubahan tak dikehendaki.

Mekanisme yang paling banyak dipakai untuk melindungi keutuhan data adalah dengan *hash* dan backup. Dengan *hash* kita dapat meyakinkan bahwa suatu data tidak diubah oleh pihak yang tidak berwenang. *Backup* adalah data cadangan, yang dipakai untuk memulihkan data ketika terjadi kerusakan karena masalah apa pun.

Ketersediaan

Serangan atas ketersediaan data yang sering muncul akhir-akhir ini adalah ransomware. Penyerang mengakses data Anda, mengenkripsinya, meletakkan data terenkripsi di lokasi yang sama dengan data asli, dan menghapus data asli. Kemudian penyerang meminta tebusan agar pemilik data asli bisa membuka data terenkripsi tersebut. Tindakan pencegahan atas serangan ransomware ini adalah backup, yang diletakkan di tempat yang memiliki kendali akses berbeda dengan data asli.

Dinamika perjalanan data memerlukan perhatian karena situasi yang berbeda juga memerlukan cara penanganan yang tepat. Data dalam keadaan tersimpan (*data at rest*) berada di berbagai media penyimpanan: berkas yang disimpan di hard disk desktop, laptop, atau server; berkas yang disimpan di diska eksternal atau diska batang. Fokus perlindungan adalah proteksi media penyimpanan, misalnya dengan enkripsi. Data dalam perjalanan (*data in transit*) melewati berbagai media komunikasi: konten atau lampiran email, konten atau berkas pesan instan, berkas yang sedang diunggah ke atau diunduh dari cloud storage, dsb. Fokus perlindungan adalah proteksi media komunikasi, misalnya memastikan bahwa akses ke server memakai protokol secure HTTP (HTTPS).

Klasifikasi Data

Selain konsep CIA untuk keamanan data, perlu juga acuan mengenai pengklaisifkasian data. Acuan bersama yang dapat dijadikan patokan adalah regulasi terkait UU PDP atau GDPR.

TAHAPAN

Terdapat tiga tujuan dalam proses penilaian data, yaitu, mengidentifikasi data sensitif dan privat, mengenali risiko dan konsekuensi kehilangan/penyalahgunaan data, serta menilai penggunaan layanan pihak ketiga.

Data sensitif dan privat

Seiring berjalannya waktu, data dan metadata yang berkaitan dengan organisasi beserta anggotanya akan sulit dikelola. Terlebih, jika suatu staf atau program menggunakan aplikasi atau layanan pihak ketiga, seperti Google Drive, OneDrive, Dropbox. Hal tersebut bisa dibilang lumrah, akan tetapi, sangat penting untuk mengelola dan mencatat di mana dan siapa saja yang bisa mengakses data tentang organisasi.

Pengaturan hak akses, tentang siapa saja yang dapat mengakses data sangat penting dilakukan dan dicek secara berkala. Proses ini juga tidak terpaku pada aplikasi atau layanan pihak ketiga di atas, tetapi pada platform yang organisasi kontrol sendiri. Misalnya situs web, NAS, dan sebagainya. Perlunya manajemen hak akses, sehingga upaya pembatasan bisa dilakukan untuk memitigasi data yang diakses oleh orang yang bukan haknya.

Risiko dan konsekuensi kehilangan/penyalahgunaan data

Identifikasi risiko dan dampak yang mungkin terjadi jika data organisasi hilang atau bocor. Tahap ini memastikan bahwa organisasi mempunyai kesadaran tentang bagaimana mereka mengelola data.

Tahapan untuk mengenali risiko dan konsekuensi adalah dengan memetakan dahulu data apa saja yang organisasi miliki. Selain pemetaan, perlu juga klasifikasi atau mengurutkan data berdasarkan tingkat kepentingan atau sensitivitasnya. Pada proses ini, organisasi

perlu juga merefleksikan bagaimana jika suatu data hilang atau terjadi penyalahgunaan data. Perlu ditimbang, seberapa besar upaya yang telah dicurahkan untuk mengumpulkan data, apabila data tersebut rusak atau hilang, apakah masih mungkin untuk dipulihkan, dan seberapa besar sumber daya (waktu, orang, biaya) untuk memulihkannya.

Penggunaan layanan pihak ketiga

Pada saat proses penilaian organisasi, auditor biasa menemui penggunaan layanan pihak ketiga. Organisasi sangat mungkin menyimpan data atau bergantung terhadap layanan terkait. Perlu pertimbangan tentang Syarat dan Ketentuan serta Kebijakan Privasi layanan terkait, sebagai bahan penilaian risiko terhadap organisasi.

Di berbagai organisasi penggunaan atau kebergantungan terhadap platform atau layanan pihak ketiga hampir sering terjadi. Selain kebijakan terkait, perlu juga melihat rekam jejak bagaimana layanan tertentu merespons, jika ada, insiden keamanan atau kebijakan mereka sendiri, khususnya terkait privasi.

PERTANYAAN

Untuk mencari tahu penggunaan data pada organisasi, auditor bisa menanyai hal-hal berikut.

- Data apa yang dianggap penting dan harus tersedia secara publik?
- Apakah ada pencadangannya (*back up*) pada data tersebut?
- Apa saja data yang dianggap privat atau rahasia organisasi?
- Bagaimana lembaga menentukan siapa yang bisa mengakses data tersebut?
- Adakah orang yang tidak punya wewenang untuk mengakses data tersebut, tetapi bisa mengaksesnya?
- Apakah staf sudah punya kriteria apa yang termasuk dalam

data sensitif?

- Data apa saja yang bisa diakses staf untuk melakukan pekerjaannya?
- Dari mana data tersebut berasal?
- Apa yang Anda lakukan terhadap data yang tidak diperlukan atau digunakan?

TINDAK LANJUT

Pertanyaan tersebut dapat menjawab bagaimana kondisi pengelolaan data dalam organisasi, sebagai metode lanjutan, Auditor bisa melakukan 4 tahap praktis untuk memetakan pengelolaan data dalam organisasi:

- Identifikasi
  Pada kerja-kerja yang dijalani organisasi, apa saja data yang dikumpulkan?
- Kelompokkan
  Kelompokkanlah data-data yang terkumpul berdasar tempat penyimpanannya. Tempat ini bisa berupa ruang fisik maupun digital. Misalnya, catatan pada buku yang tersimpan di suatu tempat, maupun informasi data pribadi dalam fail/dokumen di Google Docs atau flash disk.
- Klasifikasi
  Klasifikasilah informasi yang terkandung dalam data tersebut. Apakah isinya memuat hal sensitif, pribadi, atau privat? Sensitivitas kepentingan data ini bisa dibagi menjadi tiga kelompok: tinggi, sedang, dan rendah.
- Refleksi
  Coba pikirkan konsekuensi dan kemungkinan penyalahgunaan yang mungkin muncul.

Sebagai bahan referensi, tabel penilaian aset digital, terdapat pada Lampiran, bisa dijadikan acuan untuk melakukan pemetaan data.

Perlu diingat pula bahwa di dunia digital, pencurian data dapat dilakukan dengan menyalin, sehingga data asli seolah tidak berubah, berpindah, rusak, atau hilang. Berbeda dengan pencurian di dunia nyata, di mana benda yang dicuri berpindah tempat dan mudah terlihat dicuri atau tidaknya dari keberadaannya.

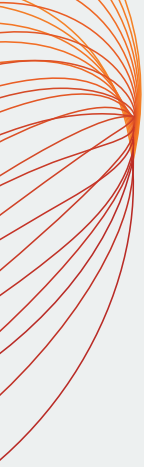
Keluaran yang diharapkan

- Daftar penggunaan layanan/platform pihak ketiga yang digunakan
- Pemetaan data dan metadata, dan hak ases pada layanan pihak ketiga.

ACUAN

Activities SAFETAG terkait:

- Sensitive Data
  https://safetag.org/activities/sensitive_data/
- Risk of Data Lost and Found
  https://safetag.org/activities/data_lost_and_found/
- Assessing Usage of Cloud Services
  https://safetag.org/activities/cloud_services/
- The Impacts of a Lost Device
  https://safetag.org/activities/impact_lost_device/
- The Impacts of a “Found” Device
  https://safetag.org/activities/impact_found_device/
- Private Data
  https://safetag.org/activities/private_data/



Materi 4:

Pemetaan Aset dan Jaringan

RINGKASAN

Aset-aset digital adalah semua perangkat yang dimiliki lembaga baik dalam bentuk perangkat keras, perangkat lunak, maupun akun-akun media sosial. Perangkat keras bisa berupa komputer, laptop, dan ponsel. Perangkat lunak mencakup sistem operasi, program, dan aplikasi yang digunakan. Sedangkan media sosial termasuk X (Twitter), Instagram, Facebook, dan Youtube.

Layaknya ketika ingin mengetahui tata letak/arsitektur bangunan, kita perlu memetakan informasi di mana saja gerbang, pagar, pintu, dan jendela yang terdapat pada bangunan tersebut. Proses identifikasi tersebut harus dilalui, sehingga kita dapat mengetahui jalan mana yang akan kita telusuri.

Selain itu kita juga akan melakukan observasi media sosial. Pengamatan media sosial diperlukan sebagai bahan tinjauan untuk mengetahui informasi apa saja yang tersedia secara publik. Setiap akun media sosial dapat dilihat dari segi keaktifannya dan ragam informasi atau konten yang termuat. Pengamatan dari sisi *username* pun diperlukan sebagai bahan identifikasi mengenai apakah ada akun tiruan atau impersonasi yang menggunakan nama lembaga. Entah menggunakanan *typosquatting* (Penyalahgunaan nama dengan kesalahan eja), akun tidak resmi yang mengatasnamakan lembaga, atau akun lama yang sudah tidak aktif.

TAHAPAN

Terdapat dua tahapan yang bisa dilalui untuk memetakan aset dan jaringan, sebagai berikut.

Observasi Media Sosial

Pada media sosial populer, coba telusuri akun-akun identik dengan nama lembaga, maupun akun resmi organisasi. Kemudian, cari tahu organisasi aktif pada media sosial apa. Selain itu, bagaimana organisasi memuat konten untuk publik bisa jadi bahan pengamatan.

No	Platform Media Sosial	Username	URL Akun	Keterangan (Contoh)
1		[nama_pengguna]	https://www.instagram.com/[nama_pengguna]	*Akun lembaga untuk berbagi foto dan video sehari-hari*
2		[nama_pengguna]	https://www.facebook.com/[nama_pengguna]	*Halaman lembaga untuk mempromosikan produk/jasa*
3		[nama_pengguna]	https://twitter.com/[nama_pengguna]	*Akun untuk berbagi berita dan update terbaru*
4		[nama_profil]	https://linkedin.com/[nama_profil]	*Profil profesional untuk networking dan mencari pekerjaan*
5		[nama_channel]	https://www.youtube.com/[nama_channel]	*Channel untuk berbagi video tutorial dan konten kreatif*

6		@[nama_peng-guna]	https://www.tiktok.com/@[nama_pengguna]	*Akun untuk membuat dan berbagi video pendek*

Pemetaan Jaringan Internal dan Eksternal

Memastikan keamanan jaringan bisa diawali dengan mengenali kondisi penggunaan jaringan organisasi. Misalnya, mengenali perangkat apa saja yang terhubung dalam jaringan internal. Kemudian, mengidentifikasi layanan organisasi apa saja yang bisa diakses secara publik. Selanjutnya, bagaimana kondisi pengaturan keamanan perangkat atau layanan terkait.

Umumnya, beberapa perangkat jaringan yang terdapat dalam suatu organisasi seperti:

- router
- switch
- network printer
- access point Wi-Fi
- NAS (LAN file storage/file sharing)
- network projector (yang tersambung melalui Wi-Fi)
- modem broadband
- smart TV
- Mikrotik
- Jaringan internet yang terbuhung dalam domain

Perangkat non jaringan yang mungkin menyimpan data sensitif

- mesin fotokopi (mungkin memilik hard disk)

Perangkat lunak yang dapat dimanfaatkan untuk pemantauan / pengendalian jarak jauh

- TeamViewer
- Remote Desktop
- VNC

- AnyDesk
- dsb.

War-Driving & War-Walking

War-Driving dan ***War-Walking*** merupakan suatu kegiatan untuk mendeteksi dan memetakan jaringan Wi-Fi dari lokasi fisik tertentu. Pemetaan dan pendeteksian dapat dilakukan menggunakan perangkat seperti smartphone atau laptop dengan cara menentukan lokasi dan ketersediaan jaringan Wi-Fi dari area sekitarnya. Perbedaannya, *War-Driving* dapat dilakukan sambil berkendaraan, sedangkan *War-Walking* dapat dilakukan sambil berjalan kaki.

Dengan melakukan *war-driving* atau *war walking*, kita dapat memperoleh informasi yang sangat berharga terkait dengan Wi-Fi yang dapat diakses dari lokasi fisik manapun. Berikut beberapa tabel panduan untuk melakukan penilaian dan pemindaan pada Wifi kantor.

No	Pertanyaan	Keterangan	Kegiatan
1	Perangkat	Apakah perangkat yang digunakan mendukung frekuensi 2.4 GHz, 5 GHz, dan 6 GHz?	Melakukan pemindaan dengan Fing atau Wifi Analyzer.
2	Wi-Fi Organisasi	Apakah ada Wi-Fi organisasi yang dapat diakses dari luar area yang seharusnya?	Melakukan pemindaan dengan Fing atau Wifi Analyzer.
		Apakah ada potensi risiko akses tidak sah atau serangan terhadap Wi-Fi organisasi?	Melakukan pengamatan perangkat terhubung melalui Fing.

		Apakah ada perangkat yang terhubung melalui kabel LAN maupun tanpa kabel?	Melakukan pemantauan kabel maupun perangkat yang terhubung dengan Wifi menggunakan Nmap atau Fing.
3	Wi-Fi Non-Organisasi	Apakah ada Wi-Fi non-organisasi yang dapat dimanfaatkan di dalam area organisasi?	Melakukan pemindaian dengan Fing atau Wifi Analyzer.
		Apakah ada risiko penyerang meninggalkan perangkat yang terhubung ke Wi-Fi luar?	Melakukan observasi di sekitar lokasi penempatan akses poin dan memeriksa kabel yang terhubung dengan router.
4	Pengumpulan Data	Apakah data hasil war driving/war walking sudah dikumpulkan secara lengkap?	Melakukan sambil melakukan pemindaan dan pengamatan melalui aplikasi Fing atau Wifi Analyzer.

Observasi dan pemeriksaan pengelolaan jaringan kantor

Kunjungan kantor merupakan salah satu kegiatan yang dilakukan tim audit keamanan digital ketika melakukan audit keamanan digital lembaga dampingan atau penerima layanan (klien). Tujuan utama kunjungan ini untuk melakukan pengamatan langsung (observasi) praktik pengelolaan jaringan kantor mitra tersebut.

Daftar Periksa

Komponen	Temuan	Kegiatan
Perangkat komputer atau laptop	Amati penggunaan perangkat staf, original atau tidak? Bagaimana kondisi perangkat? Tempatnya di mana? Pada saat kantor ditutup apakah perangkat dibawa pulang atau ditinggal?	Pengamatan

	Amati bagaimana para staf menjaga perangkatnya. Apakah ditinggal begitu saja saat ditinggalkan atau dikunci? Apa saja pengamanannya?	Pengamatan
Sistem Operasi	Amati atau tanya sistem Operasi apa saja yang digunakan oleh staf. Apakah Sistem Operasinya berlisensi sah atau tidak?	Pengamatan/ Pengecekan Perangkat
WiFi Kantor	Apakah nama SSID dan kata sandinya diberitahukan secara terbuka atau tidak. Misalnya, di dinding atau ditulis di papan?	Pengujian dengan aplikasi penangkap WiFi. Misalnya dengan menggunakan Wifi Analyzer.
	Jika nama SSID dan kata sandi tidak terbuka, mintalah kepada staf di kantor tersebut.	Meminta akses
	Cari informasi apa layanan jasa Internet yang digunakan lewat platform speedtest.net, fast.com, atau whoer.net.	Pengujian dengan platform
	Setelah menemukan layanan jasa Internet yang digunakan, cobalah masuk sebagai admin WiFi tersebut. Gunakan user dan kata sandi default. Jika menemukan masih menggunakan default, catat sebagai temuan.	Pengujian dengan mengakses
	Jika bisa masuk sebagai admin WiFi kantor mitra, catat sebagai temuan penting karena risikonya sangat tinggi.	Pengujian dengan mengakses dasbor router
	Ambil gambar untuk semua temuan, seperti nama SSID dan kata sandi yang ditempel, posisi jeroan admin WiFi lembaga, dan informasi lain-lain yang relevan.	Dokumentasi
	Tanyakan informasi pendukung lain, termasuk kapan kata sandi diganti terakhir kali, bagaimana pengaturan SSID-nya, apakah ada admin yang memantau penggunaannya, dst.	Wawancara & Pengamatan

Local Area Network (LAN)	Tanyakan apakah kantor memakai LAN atau tidak. Jika memakai, siapa saja yang bisa mengakses? Apakah tamu bisa langsung mengakesnya juga?	Wawancara & Pengamatan
Router	Tanyakan di mana letak router. Perhatikan apakah bisa diakses orang lain dengan mudah atau tidak.	Wawancara & Pengamatan
Media Penyimpanan	Apakah lembaga memiliki media penyimpanan terpusat, seperti server atau NAS? Jika punya, di mana posisinya? Siapa saja yang bisa mengakses ruangan ataupun jaringannya, lokal atau bisa dari jarak jauh?	Wawancara & Pengamatan
Jaringan	Jika menggunakan pihak ketiga untuk mengatur WIFI, LAN, NAS, dsb, siapa pihak ketiga tersebut? Bagaimana statusnya (konsultan atau seperti apa?) Apa latar belakang pihak ketiga tersebut? Adakah narahubung dari staf kantor untuk transfer info atau pengetahuan dari konsultan?	Wawancara
Perangkat terhubung	Melakukan pemindaan dengan aplikasi atau melalui dashboard router untuk memastikan perangkat terhubung dikenali.	Pengujian dengan aplikasi Fing atau Nmap
Kamera Pengawas	Perhatikan apakah kantor memiliki kamera pengawas (CCTV)? Berapa? Bagaimana penempatannya?	Pengamatan
Keamanan Fisik Lain	Ada beberapa hal lain yang juga perlu diperhatikan. Meskipun bukan termasuk keamanan digital, tetapi aspek-aspek berikut berpengaruh juga pada keamanan digital, yaitu lingkungan sekitar, pagar kantor, pengaturan ruangan, penanggung jawab keamanan, posisi duduk, dan lain-lain.	

DAFTAR PERIKSA

Pemeriksaan dapat dilakukan dengan cara observasi dan mengisi daftar pertanyaan berikut ini:

No	Pertanyaan	Jawaban (Ya/Tidak)	Catatan/ Temuan
1	Apakah halaman admin dari router memakai kredensial bawaan atau default?		
2	Apakah terdapat perangkat tidak dikenali yang terhubung dalam jaringan?		
3	Situs atau layanan apa saja yang dapat diakses secara publik?		
4	Apakah semua perangkat jaringan dan non-jaringan telah diperbarui ke versi terbaru?		
5	Apakah ada kebijakan penggunaan password yang kuat dan diterapkan secara konsisten?		
6	Apakah ada sistem deteksi intrusi (IDS) atau sistem pencegahan intrusi (IPS) yang aktif?		
7	Apakah ada firewall yang melindungi jaringan dari akses yang tidak sah?		

DAFTAR PERTANYAAN

Pertanyaan yang bisa dilontarkan untuk tahap ini adalah:

No	Pertanyaan	Jawaban (Ya/Tidak)	Catatan/ Temuan
1	Apakah tahu cara mengakses halaman admin dari router?		
2	Apakah masih memakai kredensial bawaan atau default?		
3	Siapa yang bisa mengakses halaman admin dari router?		
4	Apakah menggunakan Mikrotik atau perangkat pengatur layanan jaringan?		

5	Apakah ada layanan yang tersedia dalam jaringan yang tidak diberi tahu oleh staf organisasi?		
6	Apa sistem operasi, atau layanan/aplikasi yang digunakan organisasi? Apakah ada hal tidak umum, berbeda, atau belum diperbarui mengenai layanan atau sistem operasi yang dijalankan?		
7	Apakah semua perangkat jaringan dan non-jaringan telah diperbarui ke versi terbaru?		
8	Apakah ada kebijakan penggunaan password yang kuat dan diterapkan secara konsisten?		
9	Apakah ada firewall yang melindungi jaringan dari akses yang tidak sah?		
10	Apakah ada backup data yang dilakukan secara teratur?		
11	Apakah karyawan diberi pelatihan keamanan secara cukup?		
12	Apakah ada kebijakan penggunaan yang jelas untuk perangkat pribadi yang terhubung ke jaringan organisasi?		

Untuk membantu memetakan aset dan jaringan, layanan pihak ketiga berikut bisa digunakan.

- Pemetaan Jaringan eksternal atau publik: https://dnsdumpster.com/
- Identifikasi perangkat yang terhubung dalam jaringan internal: Fing atau Nmap

TINDAK LANJUT

Jangan lupa bahwa perangkat jaringan (router, switch, modem, dll.), terutama yang manageable, boleh jadi juga dapat dimutakhirkan *firmware*-nya.

Keluaran yang diharapkan

Berdasarkan penilaian ini hasil yang akan didapatkan adalah sebagai berikut:

- Daftar hasil dokumentasi observasi media sosial.
- Data pemetaan jaringan internal dan eksternal.
- Data dokumentasi observasi dan pemeriksaan pengelolaan jaringan kantor.
- Data dokumentasi observasi dan pemeriksaan pengelolaan Wifi.
- Informasi dokumentasi hasil wawancara.

ACUAN

Activities SAFETAG terkait:

- Network Scanning
  https://safetag.org/activities/network_scanning
- Network Access
  https://safetag.org/activities/network_access
- Network Traffic Analysis
  https://safetag.org/activities/traffic_analysis
- Remote Network and User Device Assessment
  https://safetag.org/activities/remote_network_device_assessment
- Router Based Attacks
  https://safetag.org/activities/router_attacks
- VoIP Security Assessment
  https://safetag.org/activities/voip_assessment
- Wireless Range Mapping
  https://safetag.org/activities/wireless_range_mapping
- Monitor Open Wireless Traffic
  https://safetag.org/activities/monitor_open_wireless_traffic

Materi 5:

Pemindaian dan Analisis Kerentanan

RINGKASAN

Pada tahap ini auditor mencari kemungkinan celah keamanan dalam perangkat, layanan, aplikasi, dan jaringan organisasi dengan menguji dan membandingkannya dengan berbagai sumber (databases kerentanan, informasi vendor/layanan, dan investigasi/ temuan audit).

Dalam melakukan pemindaian kerentanan, perlu kita bedakan mengenai Asesmen Kerentanan dan Uji Penetrasi. Asesmen kerentanan lebih bersifat menyeluruh, sedangkan Uji Penetrasi lebih mendalam. Kedua hal tersebut juga memiliki tujuan yang berberda. Asesmen kerentanan bertujuan untuk melihat sejauh mana kerentanan dapat muncul atau potensial bersarang pada suatu sistem organisasi. Di sisi lain, Uji Penetrasi lebih berfungsi untuk memverifikasi suatu kerentanan dan memiliki tujuan yang spesifik.

Dalam proses pemindaian kerentanan, penggunaan aplikasi non-teknis dapat dimanfaatkan, tetapi penggunaan aplikasi harus didasarkan pada pemahaman tentang batasan, lingkup, dan konsekuensi dari pemindaian oleh aplikasi atau layanan pihak ketiga terkait, terutama jika berbasis web. Sebagai contoh, penggunaan aplikasi layanan pihak ketiga tidak dapat memindai sedalam dan sejauh aplikasi teknis khusus. Penggunaannya hanya sebatas memindai di dasarnya saja.

Untuk mendapatkan pemindaian yang lebih komprehensif, perlu

menggunakan aplikasi khusus, seperti Burp Suite, Nessus atau beberapa aplikasi alternatif lainnya. Namun, sebagaian besar penggunaan aplikasi tersebut memerlukan pemahaman dan keahlian teknis yang lebih mendalam.

Terakhir, analisis PAKEM DIRI untuk melihat penerapan perilaku atau kebijakan keamanan digital dan praktik keamanan apa saja yang belum diterapkan sehingga mempengaruhi keamanan digital organisasi.

TAHAPAN
Mengenali dan Memindai Situs Web

Website footprinting

Website footprinting merupakan sebuah proses mencari tahu dan menemukan segala sesuatu mengenai suatu situs web atau domain, termasuk informasi berupa servernya, teknologi yang digunakan, dan data lainnya yang mungkin berguna bagi penyerang. Kata *footprinting* sendiri mengacu pada istilah teknis dalam dunia komputer terkait proses untuk memperoleh informasi mengenai suatu sistem atau jaringan.

Menggunakan alat pindai berbasis layanan pihak ketiga sebagai langkah awal adalah hal yang dapat dilakukan untuk mengumpulkan informasi mengenai suatu situs web dan memulai Asesmen Kerentanan pada situs tersebut.

Contohnya, ketika terdapat temuan direktori situs web yang yang bisa diakses secara publik, segala informasi dapat dikumpulkan untuk mengenali karakteristik situs web. Misalnya apakah terdapat suatu temuan (informasi, file, aplikasi) yang mengandung informasi sensitif (kata sandi, konfigurasi aplikasi) atau aplikasi yang rentan atau belum diperbaharui.

Beberapa layanan berbasis web yang dapat digunakan untuk menunjang praktik ini adalah:

- Builtwith https://builtwith.com/
- DNSDumpster https://dnsdumpster.com/
- MX Lookup Tool https://mxtoolbox.com/
- SecurityTrails https://securitytrails.com
- Censys https://search.censys.io/

Data yang dikumpulkan menjadi modal utama sebagai informasi untuk menyesuaikan langkah selanjutnya. Misalnya, penggunaan situs web berbasis WordPress perlu menyesesuaikan alat pemindai yang digunakan menjadi WPScan. Atau situs web yang dibangun dengan teknologi terbaru, perlu melakukan pemindaian dari sisi aplikasi web dan API-nya (*Application Programming Interface*).

Pemindaian Kerentanan

Pemindaian situs web dilakukan untuk melihat kondisi dan gambaran umum postur keamanan situs web. Selain itu, pengecekan terhadap temuan kerentanan perlu untuk memastikan situs web tidak terinfeksi.

Trend terkini serangan ke web adalah dengan menitipkan beberapa halaman tambahan, khususnya ini biasa dilakukan oleh situs judi online. Mereka melakukan ini dengan harapan bahwa seluruh domain tidak diblokir karena memang berasal dari situs legitimate, sehingga beberapa halaman sisipan tersebut akan bisa bertahan keberadaannya.

Penyerang yang melakukan hal ini biasanya telah meninggalkan *backdoor* sehingga walau sekadar menghapus halaman-halaman sisipan tersebut, mereka dengan cepat dapat menambahkan lagi halaman-halaman sisipan baru. Maka, penanganan kasus ini perlu direncanakan dengan masuk ke dalam sistem dan perlu memastikan

bahwa penyerang tidak bisa masuk lagi.

Beberapa aplikasi atau layanan yang dapat digunakan untuk memindai kerentanan, sebagai berikut.

- WPScan https://wpscan.com/
- Securi https://sitecheck.sucuri.net/
- UpGuard https://webscan.upguard.com/
- SSLabs Test https://www.ssllabs.com/ssltest/
- Nikto https://github.com/sullo/nikto
- Nessus atau Burp Suite
- Daftar aplikasi pemindai kerentanan OWASP

Beberapa aspek pertanyaan yang bisa dipertimbangkan adalah:

No	Pertanyaan	Jawaban (Ya/Tidak)	Catatan/ Temuan
1	Apakah situs-situs web organisasi telah mengimplementasikan protokol HTTPS (TLS/ SSL) dengan baik?		
2	Apakah situs web terdaftar pada daftar hitam?		
3	Apakah hasil pemindaian menunjukan kerentanan?		
4	Bagaimana kondisi pengamanan infrastruktur surel organisasi?		

Pemindaian melalui layanan pihak ketiga berikut bisa membantu beberapa tahapan proses ini.

1. Mengidentifikasi Target dengan mentukan website yang akan diuji.
2. Menggunakan BuiltWith untuk mengenali teknologi yang digunakan.
3. Menggunakan DNSDumpster dan SecurityTrails untuk meme-

takan infrastrukturnya.

4. Menggunakan WPScan (jika relevan) untuk memindai kerentanan website yang berbasis pada WordPress.
5. Menggunakan Sucuri untuk melakukan pemindaian situs web.
6. Menggunakan SSLabs untuk memeriksa konfigurasi SSL/TLS.
7. Menggunakan UpGuard mencari kerentanan.
8. Jika memiliki kemampuan lebih teknis lakukan Penetration Testing: Verifikasi kerentanan.
9. Membuat Laporan dari dokumentasikan temuan dari pengujian sebelumnya.

Berikut ini daftar fungsi layanan pengujian pihak ketiga yang dapat digunakan.

Alat	Kategori	Fungsi Utama	Kegunaan Utama
BuiltWith	Pembaca Teknologi Website	Mengidentifikasi teknologi yang digunakan dalam membangun situs web	Mengidentifikasi informasi bagaimana suatu situs web dibangun
DNSDumpster	Pencari Subdomain dan Informasi DNS	Mencari subdomain, IP alamat, dan informasi DNS lainnya	Menemukan informasi jaringan terkait pada suatu domain
SecurityTrails	Pencari Subdomain dan Informasi DNS	Menyediakan data tentang infrastruktur digital	Serupa dengan DNSDumpster, tetapi menawarkan fitur yang lebih lengkap
WPScan	Pembaca Kerentanan Umum	Khusus untuk memindai kerentanan pada situs WordPress	Mengidentifikasi kerentanan yang spesifik pada platform WordPress

Sucuri	Pembaca Kerentanan Umum	Menyediakan platform untuk penilaian keamanan web secara umum	Mengidentifikasi kerentanan umum pada suatu situs web
UpGuard	Pemantau Keamanan dan Kepatuhan	Menyediakan platform untuk penilaian keamanan web secara umum	Mengidentifikasi kerentanan umum pada suatu situs web
SSL Labs	Penguji Sertifikat SSL	Menganalisis konfigurasi SSL/TLS pada sebuah server web	Memastikan konfigurasi SSL/TLS aman dan sesuai dengan praktik terbaik

Analisis PAKEM DIRI

PAKEM DIRI merupakan metode penilaian risiko keamanan secara mandiri yang dikembangkan SAFEnet. Ada 50 pertanyaan yang terdiri dari empat komponen keamanan digital, yaitu keamanan perangkat, identitas, komunikasi, dan ponsel. Pengisi PAKEM DIRI hanya perlu menjawab dengan dua pilihan jawaban, Ya atau Tidak, merujuk pada perilaku keamanan yang sudah diterapkan.

Hingga saat ini, ada dua metode pengisian PAKEM DIRI, yaitu secara daring dan luring. Masing-masing metode memiliki keuntungan sendiri. Untuk metode daring, pengisian bisa langsung dilakukan melalui platform pakemdiri.safenet.or.id. Keuntungan pengisian secara daring ini karena bisa dilakukan lebih spesifik per komponen keamanan. Hasilnya otomatis terlihat dalam bentuk persentase setelah mengisi. Pengisian juga bisa dipilih apakah hanya komponen tertentu atau semua komponen.

Adapun metode luring dilakukan melalui pengisian formulir dalam format tabel (sheet), baik .ods untuk LibreOffice maupun .xls untuk Excel. Formulir PAKEM DIRI ada di bagian lampiran panduan ini.

Keuntungan pengisian secara luring adalah karena tidak harus menggunakan internet dan bisa dikompilasi jika PAKEM DIRI tersebut sebagai bagian dari audit keamanan digital.

Untuk keperluan audit ini, kami menyarankan untuk menggunakan mengisi PAKEM DIRI secara luring. Hasil tiap orang kemudian akan dijumlahkan secara total untuk kemudian dibagi jumlah pengisi sehingga diperoleh nilai rata-rata PAKEM DIRI untuk organisasi yang diaudit. Tingkat risikonya bisa dilihat dari nilai rata-rata tersebut merujuk kepada kategori risiko yang ada di bagian bawah formulir PAKEM DIRI. Dari sini, hasil PAKEM DIRI bisa menggambarkan postur keamanan digital organisasi.

Analisis lanjutan yang perlu dilakukan adalah melihat di bagian mana dari tiap komponen dan perilaku yang perlu mendapat perhatian lebih tinggi karena berisiko sangat tinggi atau tinggi. Hal ini bisa dilihat dari nilai rata-rata atau persentase paling rendah karena menunjukkan sedikitnya staf yang menerapkan perilaku keamanan digital tersebut. Contohnya, persentase yang menerapkan di bawah 30%, maka hal itu menunjukkan bahwa sangat sedikit staf yang menerapkannya sehingga risiko keamanan digital pada perilaku tersebut relatif tinggi sehingga perlu mendapatkan perhatian lebih lanjut.

Berdasarkan temuan tersebut, auditor bisa memberikan rekomendasi sesuai perilaku keamanan yang belum banyak diterapkan tersebut.

TINDAK LANJUT
Keluaran yang diharapkan

Berdasarkan penilaian ini hasil yang akan didapatkan adalah sebagai berikut:

- Nilai rata-rata PAKEM DIRI
- Data hasil pemindaan Subdomain dan Informasi DNS
- Data hasil pemindaan kerentanan.
- Data hasil pengecekan Penguji Sertifikat SSL

ACUAN

Activities SAFETAG terkait:

- Vulnerability Scanning
  https://safetag.org/activities/vulnerability_scanning/
- Vulnerability Research
  https://safetag.org/activities/vulnerability_research/
- Website Footprinting
  https://safetag.org/activities/web_footprint/
- Web Vulnerability Assessment
  https://safetag.org/activities/web_vulnerability_assessment/
- VoIP Security Assessment
  https://safetag.org/activities/voip_assessment/
- Check Config Files
  https://safetag.org/activities/check_config_files/
- Router Based Attacks
  https://safetag.org/activities/router_attacks/

Materi 6:
Penilaian Kapasitas Organisasi

RINGKASAN

Kapasitas sebuah organisasi akan menentukan sejauh mana mereka bisa melakukan mitigasi terhadap ancaman dan serangan digital. Sebab itu penting untuk mengetahui sejauh mana modal dan sumber daya organisasi dalam keamanan digital, termasuk kebijakan, keahlian, keuangan, kemauan untuk belajar, waktu staf, dan lain-lain.

Ada tiga aspek yang digunakan dalam menilai kapasitas keamanan digital sebuah organisasi yang biasa disebut 3P, yaitu *process* (kebijakan), *people* (manusia), dan *platform* (teknologi yang digunakan). Ketiga aspek tersebut dilihat dari perspektif keamanan digital.

Aspek kebijakan, misalnya, menjadi acuan dalam menilai kapasitas dengan melihat apakah organisasi sudah memiliki kebijakan keamanan digital atau tidak. Jika sudah memiliki, apakah sudah diterapkan dengan baik atau tidak. Aspek ini juga mencakup penyediaan staf dan keuangan oleh organisasi.

Aspek manusia berfokus pada sumber daya manusia sebagai aset utama organisasi. Sumber daya manusia berkaitan dengan pengetahuan dan keterampilan yang dimiliki staf organisasi baik kemampuan teknis maupun non-teknis untuk menilai kapasitas keamanan digital organisasi.

Adapun aspek teknologi menyangkut teknologi apa yang digunakan

oleh organisasi dan stafnya. Misalnya, apakah teknologi tersebut menggunakan sistem operasi di laptop staf orisinil atau bajakan. Jika orisinil, apakah sudah menggunakan versi terbaru atau sudah ketinggalan.

Dengan menilai kapasitas keamanan digital suatu organisasi, maka memungkinkan auditor untuk memberikan rekomendasi lebih tepat sehingga peluang untuk diterapkan oleh organisasi yang diaudit juga lebih besar.

TAHAPAN

Mengacu kepada tiga aspek untuk menilai kapasitas keamanan digital organisasi yang diaudit sebagaimana disebutkan di atas, maka tahapan penilaian pun dibagi dalam tiga aspek tersebut, yaitu kebijakan, manusia, dan teknologi. Tiap aspek perlu dikaji lebih lanjut pada saat wawancara dan observasi langsung.

Kebijakan

Pertanyaan terkait kebijakan organisasi mencakup hal-hak berikut:

- Apakah organisasi sudah memiliki kebijakan keamanan digital?
- Jika sudah ada, apa saja isinya dan sejauh mana penerapannya?
- Siapa yang bertanggung jawab terhadap keamanan digital organisasi?
- Jika tidak ada staf khusus, bagian atau divisi apa yang paling relevan dengan keamanan digital?
- Bagaimana kemauan organisasi, terutama pimpinannya, untuk mengadopsi teknologi atau praktik baru?
- Sumber daya apa saja yang dimiliki dan disediakan organisasi untuk keamanan digital, misalnya pendanaan atau staf yang berpengalaman?

- Bagaimana hubungan organisasi dengan pihak lain yang berpengalaman dalam keamanan digital selama ini?
- Apakah organisasi bisa dengan mudah mengakses bantuan, baik penanganan ataupun pendanaan, jika mengalami serangan digital?

Manusia

Pertanyaan terkait sumber daya manusia bisa diajukan pada saat wawancara maupun observasi kantor termasuk:

- Apakah staf organisasi sudah pernah mendapatkan pelatihan keamanan digital? Jika ada, berapa persen dari total staf?
- Jika ada staf organisasi yang sudah mendapatkan pelatihan keamanan digital, sejauh mana mereka menerapkan pengetahuan dan keterampilannya untuk keamanan diri sendiri dan organisasi?
- Berapa rata-rata usia staf organisasi? Bagaimana kapasitas mereka secara umum? Meskipun tidak selalu benar, tetapi pada umumnya staf organisasi yang lebih muda akan lebih melek keamanan digital.
- Apakah ada staf yang bertanggung jawab atas sistem IT organisasi? Sejauh mana ia menguasai teknologi/keamanan digital?
- Bagaimana perilaku staf terkait keamanan digital secara umum, termasuk dalam media sosial?

Teknologi

Pertanyaan terkait teknologi yang digunakan bisa ditanyakan pada saat wawancara, tetapi sangat penting untuk dikonfirmasi pada saat observasi di kantor, termasuk hal-hal berikut:

- Apa saja perangkat keras dan perangkat lunak yang digunakan organisasi maupun stafnya?
- Sudah berapa tahun laptop yang digunakan masing-masing staf? Makin tua, biasanya makin berisiko.

- Apa jenis sistem operasi yang digunakan? Misalnya, Windows, Mac, atau Linux?
- Jika menggunakan Windows, penting sekali untuk memeriksa di perangkat apakah Windows tersebut orisinil ataukah bajakan?
- Apakah ada aplikasi atau program bajakan di perangkatnya?
- Apakah ada teknologi khusus untuk melindungi keamanan fisik dan digital organisasi maupun stafnya?

Tiap aspek memengaruhi kapasitas keamanan digital sebuah organisasi. Pada aspek kebijakan, misalnya, jika sebuah organisasi sudah memiliki kebijakan yang diterapkan dengan baik dan konsisten, termasuk penanggung jawab, maka kapasitasnya akan meningkat. Namun, jika tidak memiliki kebijakan dan staf khusus, maka kapasitasnya rendah. Pada aspek sumber daya manusia, semakin banyak staf pernah mengikuti pelatihan keamanan digital serta menerapkan dengan baik, semakin baik kapasitas organisasi tersebut. Terakhir, pada aspek teknologi, perangkat dan program yang sudah tua dan tidak diperbarui atau menggunakan bajakan tentu akan membuat kapasitasnya jadi lebih rendah dan sebaliknya.

TINDAK LANJUT

Masalah yang teridentifikasi dalam tahap ini dapat ditangani dengan berbagai cara. Aspek pertama, adalah bahwa penanganan perlu dilakukan dengan perbaikan pada satu atau lebih dari PPP (process, people, platform): proses (kebijakan dan atau prosedur), people/SDM, dan platform (perangkat keras, perangkat lunak).

Kebijakan mesti menjadi acuan semua aspek lain. Kebijakan perlu diuraikan secara lebih rinci dalam prosedur. Dari kebijakan tersebut, diturunkan kebutuhan tentang people/SDM: apakah perlu SDM baru, apakah perlu rotasi SDM, apakah perlu pelatihan dengan

topik tertentu bagi SDM yang sudah ada. Kebijakan juga mendorong langkah pemilihan platform: apakah perlu mengganti atau menambah perangkat keras yang ada, apakah perlu mengganti atau menambah perangkat lunak yang ada.

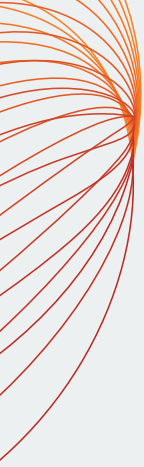
Untuk memperoleh hasil jangka panjang yang lebih baik, maka berbagai aspek keamanan ini perlu dikelola/di-manage. Ada beberapa standar yang dapat diacu untuk melaksanaan pengelolaan/manajemen keamanan IT, misalnya ISO 27001 dan/atau NIST Cyber Security Framework. Organisasi yang cukup besar dan memiliki sumber daya yang memadai dapat memilih untuk mengambil sertifikasi ISO 27001, misalnya. Organisasi yang belum memiliki sumber daya yang cukup dapat mengambil langkah upaya pemenuhan standar tersebut, tanpa mengambil sertifikasinya. Tingkat yang lebih tinggi pengelolaanya adalah dengan memperhatikan tingkat kematangan (*maturity level*). Hal ini mempersyaratkan adanya pengukuran ke berbagai aspek penilaian tingkat kematangan, dan dilakukan secara berkala.

Satu alternatif yang dapat dilakukan oleh organisasi untuk meningkatkan kapasitas adalah dengan menjalin kerja sama dengan pihak lain di bidang-bidang yang diidentifikasi kurang di dalam organisasi. Secara global, ketersediaan SDM keamanan IT kurang, sehingga untuk menambah SDM IT Security secara permanen ke suatu organisasi akan menemui banyak kendala.

ACUAN

Activities SAFETAG terkait:

- Interview https://safetag.org/activities/interviews/
- Guiding Questions for High-Risk Organisations https://safetag.org/activities/interviews_highrisk/
- Capacity Assessment Checklist https://safetag.org/activities/capacity_assessment_cheatsheet/



Materi 7:

Penyusunan dan Penyampaian Laporan

RINGKASAN

Tahap terakhir dalam proses audit SAFETAG adalah menyusun laporan. Setelah mengumpulkan seluruh informasi yang berkaitan dengan tujuan dan lingkup audit, lalu mempertimbangkan kapasitas organisasi. Auditor perlu menyusun dan merumuskan rekomendasi berdasarkan temuan-temuan yang tersedia. Dari hasil profil risiko dan ancaman yang dihadapi, proses pengelolaan data, informasi serta hasil pindai yang berkaitan dengan aset dan jaringan, hingga penilaian kebijakan atau kapasitas. Hal tersebut harus disusun secara akurat, jelas, dan konstruktif.

Bentuk laporan yang umum dipakai adalah yang memuat daftar temuan/masalah, beserta rekomendasi perbaikannya. Pada berbagai kegiatan audit, waktu yang diperlukan untuk melakukan perbaikan ini cukup bervariasi. Ketika rencana audit awal juga memasukkan tahap pemeriksaan ulang setelah perbaikan, maka waktu pelaksanaan pemeriksaan ulang ini mesti direncanakan dengan mempertimbangkan rentang waktu perbaikan di atas.

Penyusunan laporan perlu memerhatikan target audiens pembaca, sehingga penyesuaian bahasa bisa dilakukan. Hal tersebut dilakukan guna mempermudah pembaca memahami maksud dan hasil dari seluruh rangkaian kegiatan audit. Umumnya, penerima laporan bisa saja datang dari berbagai latar belakang, maka dari itu, sebaiknya penulisan laporan tidak menggunakan kata komputasi atau teknis. Jika terdapat kebutuhan tersebut, setidaknya penjelasan singkat

tentang kata terkait harus dicantumkan.

Esensinya, laporan harus dapat dicerna dengan baik dan rekomendasi bisa diterapkan oleh organisasi yang diaudit. Laporan harus didasarkan dengan tujuan mengkomunikasikan pesan auditor dengan jelas dan mengajak organisasi ke arah yang lebih baik.

Selain itu, pertimbangan terhadap preferensi organisasi dalam menerima laporan patut dipertanyakan. Ada yang menginginkan laporan komprehensif secara mendalam, ada juga yang hanya membutuhkan laporan singkat.

Satu hal lain yang harus disadari oleh organisasi adalah bahwa menjaga keamanan organisasi itu adalah suatu proses yang mesti dilakukan secara terus menerus. Dengan berjalannya waktu selalu akan ada perubahan misalnya adanya perangkat keras dan perangkat lunak baru, atau penyerang menemukan cara-cara baru untuk melakukan aktivitas mereka, yang menimbulkan ancaman baru, kerentanan baru. Praktik yang disarankan adalah untuk melakukan manajemen keamanan IT, dengan salah satu program berupa audit berkala, minimal setahun sekali.

Secara garis besar, penyusunan laporan berisi informasi umum keseluruhan rangkain audit, tetapi dalam tahap tertentu ketika terdapat informasi teknis yang berkaitan dengan proses audit, perlu juga melampirkan informasi terkait di dalam bagian laporan.

Informasi teknis sendiri dapat berupa data terkait hasil pemindaian dari berbagai aplikasi asesmen kerentanan yang sudah digunakan. Misalnya data terkait informasi jenis dan tata letak kerentanan situs web atau jaringan.

TAHAPAN
Kerangka Laporan

Jumlah catatan dan temuan selama proses rangkaian audit sangat beragam. Sebagai referensi, kerangka hasil laporan audit bisa mengacu pada informasi berikut.

- Pengantar
  - Latar Belakang
  - Tujuan
  - Ruang Lingkup
  - Metodologi
- Temuan
  - Profil lembaga
  - Risiko dan ancaman
  - Kapasitas
  - Jaringan dan Infrastruktur
  - Aset-aset digital
- Rekomendasi
  - Kebijakan
  - Jaringan dan Infrastuktur
  - Aset-aset digital
- Penutup
- Lampiran teknis terperinci atau lainnya

Selain itu, terdapat beberapa pertanyaan yang bisa dijadikan bahan pertimbangan untuk disertakan dalam proses penyusunan laporan.

- Apa kekuatan organisasi (keahlian, dana, kemauan untuk belajar, waktu staf, dsb.) yang dapat dimanfaatkan ketika terdapat proses adopsi/perubahan teknologi?
- Apa kelemahan organisasi (keahlian, dana, kemauan untuk belajar, waktu staf, dsb.) yang perlu dipertimbangkan ketika terdapat proses adopsi/perubahan teknologi?
- Apa hambatan organisasi dalam mengadopsi hal baru seperti,

kebijakan atau teknologi?

DEBRIEF

Debrief dapat dilakukan sebagai langkah terakhir setelah penyampaian laporan audit secara tertulis. Pertemuan terakhir dapat dilakukan untuk memaparkan atau memberikan informasi relevan mengenai serangkaian langkah apa saja yang telah dilalui, temuan utama, serta temuan lainnya yang memerlukan perhatian lebih.

Tahap ini merupakan waktu yang pas juga bagi organisasi yang diaudit untuk menanyakan lebih lanjut segalah hal terkait keseluruhan rangkaian proses audit ataupun hal lainnya.

TINDAK LANJUT

Keluaran yang diharapkan

- Hasil dokumen laporan beserta informasi pendukung

ACUAN

Activities SAFETAG terkait:

- Creating a Risk Matrix
  https://safetag.org/activities/risk_matrix/
- Roadmap Development
  https://safetag.org/activities/roadmap_development/
- Resource Identification
  https://safetag.org/activities/identify_useful_resources/
- Report Creation https://safetag.org/activities/report_creation/
- Debrief https://safetag.org/methods/debrief/

Penutup

Keamanan digital telah menjadi aspek krusial dalam kerja-kerja organisasi masyarakat sipil di era digital ini. Melalui panduan ini, kami berharap dapat memberikan kontribusi nyata dalam meningkatkan kesadaran dan kapasitas organisasi masyarakat sipil Indonesia dalam menghadapi tantangan keamanan digital yang semakin kompleks.

Panduan ini merupakan hasil dari perjalanan panjang SAFEnet dalam melakukan audit keamanan digital sejak tahun 2021, yang telah mencakup lebih dari 50 organisasi masyarakat sipil di berbagai bidang. Dengan mengadaptasi kerangka kerja SAFETAG dan menyesuaikannya dengan konteks Indonesia, kami berupaya menyajikan materi yang relevan dan aplikatif.

Kami menyadari bahwa ancaman digital terus berkembang, dan karenanya, upaya peningkatan keamanan digital harus menjadi proses yang berkelanjutan. Panduan ini bukan hanya sebuah dokumen statis, melainkan sebuah langkah awal dalam membangun budaya keamanan digital yang kuat di kalangan organisasi masyarakat sipil.

Serta, perlu diingat bahwa panduan ini bukan solusi lengkap untuk keamanan di dunia digital, melainkan hanya salah satu cara untuk memitigasi risiko. Panduan ini mengajak pengguna melakukan proses untuk, setidaknya, mengevaluasi tentang analisis risiko dan ancaman, kapasitas organisasi, dan perilaku staf. Hal tersebut termasuk dengan teknologi yang digunakan, kapasitas sumber daya manusia, dan ada tidaknya proses atau kebijakan keamanan digital. Selain itu, panduan ini juga membahas bagaimana penerapan kebijakan tersebut jika sudah ada. Evaluasi ini perlu dilakukan secara rutin

untuk menilai kapasitas organisasi dalam menghadapi potensi risiko, ancaman, dan serangan digital yang terus berkembang dan bervariasi.

Akhir kata, semoga panduan ini dapat memberikan kontribusi yang berarti dalam menciptakan praktik keamanan digital yang lebih baik bagi OMS, untuk membangun lingkungan digital yang lebih aman dan mendukung perjuangan untuk demokrasi dan hak asasi manusia di Indonesia.

Lampiran

PAKEM DIRI

KEAMANAN PERANGKAT			
Kriteria Keamanan	**Ya**	**Tidak**	**Tingkat Risiko**
Memisahkan laptop untuk bekerja dan pribadi			
Memisahkan ponsel untuk bekerja dan pribadi			
Menggunakan sistem operasi (OS) orisinal, bukan bajakan			
Menggunakan kata sandi untuk membuka perangkat			
Mengaktifkan firewall			
Melakukan enkripsi media penyimpan			
Mematikan fungsi lokasi pada laptop			
Mematikan fungsi lokasi pada ponsel kecuali diperlukan			
Melakukan pencadangan (back up) secara berkala, setidaknya sebulan sekali			
Membersihkan berkas dan aplikasi yang sudah tidak digunakan secara berkala			
Menggunakan antivirus dan pembersih (cleaner)			
Memperbarui (update) sistem operasi dan aplikasi jika ada pembaruan			

KEAMANAN KOMUNIKASI			
Kriteria Keamanan	**Ya**	**Tidak**	**Tingkat Risiko**
Komunikasi sehari-hari menggunakan platform aman			
Komunikasi sensitif menggunakan platform aman			
Surel aman untuk berkomunikasi tentang hal-hal sensitif			
Pada saat beraktivitas daring (online) menggunakan koneksi privat yang aman			
Menghindari penggunaan informasi sensitif dan personal ketika menggunakan Wifi publik			
Menggunakan VPN ketika mengakses Wifi publik			
Menggunakan peramban aman dalam metode Private atau Incognito untuk mengurangi jejak digital saat berselancar			
Menambah add-ons atau plugin seperti Privacy Badger dan HTTPS Everywhere pada peramban			
Menggunakan Jitsi, BigBlueBotton atau layanan lain yang terenkripsi untuk video call			
Menggunakan mesin pencari yang lebih menghargai privasi			
Mewaspadai dan berhati-hati terhadap surel atau pranala dari pengirim yang tidak dikenal			
Memeriksa dulu keamanan pranala atau berkas yang diterima di email dengan database malware seperti virustotal dan urlscan.io			

KEAMANAN AKUN			
Kriteria Keamanan	**Ya**	**Tidak**	**Tingkat Risiko**
Membedakan antara akun pribadi, seperti untuk belanja dengan akun pekerjaan			
Membatasi mengunggah identitas personal seperti keluarga, tanggal lahir, alamat, dan semacamnya			
Membuat password yang kompleks dan kuat			
Membuat password berbeda-beda untuk setiap aset digital yang dimiliki			
Mencatat password di aplikasi pengelola password seperti KeePass			
Mengganti password secara berkala setidaknya enam bulan sekali			
Menggunakan metode 2FA untuk memperkuat keamanan perangkat maupun aset-aset digital lainnya			

KEAMANAN PONSEL			
Kriteria Keamanan Ponsel	**Ya**	**Tidak**	**Tingkat Risiko**
Melindungi ponsel secara fisik yaitu dengan menggunakan pelindung luar (casing) dan atau pelindung layar (screen guard)			
Melindungi ponsel dengan password atau pola agar tidak mudah diakses orang lain			

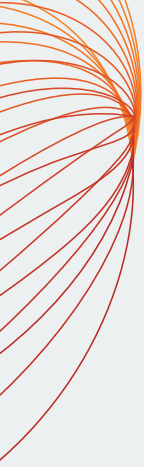
Memperbarui sistem operasi (OS) jika tersedia			
Memperbarui aplikasi jika tersedia di OS			
Mengganti nama ponsel dengan nama lain agar tidak mudah dikenali			
Menonaktifkan Bluetooth dan Wifi jika tidak sedang digunakan			
Memasang (install) aplikasi hanya dari sumber resmi			
Mengaktifkan lokasi pada ponsel hanya jika digunakan			
Keluar (logout) dari aplikasi email jika tidak digunakan dalam waktu lama, misalnya satu minggu			
Memeriksa sejauh mana akses oleh setiap aplikasi terhadap data yang ada dalam ponsel			
Memeriksa apa saja perangkat lain (misalnya laptop) yang digunakan untuk aplikasi pesan ringkas di ponsel, seperti Wire, Telegram dan WhatsApp			
Menggunakan peramban yang tidak merekam aktivitas penggunanya, seperti Firefox Focus			
Menggunakan VPN jika mengakses Wifi publik			
Melakukan pencadangan data (back up) secara berkala, misalnya sebulan sekali			
Mengaktifkan enkripsi pada ponsel agar tidak bisa dibuka dari perangkat lain tanpa izin pemilik			
Memasang aplikasi mesin pencari yang aman, seperti DuckDuckGo			

Menggunakan antivirus untuk mendeteksi jika ada perangkat berbahaya (malware) di ponsel			
Memeriksa secara berkala aplikasi dan berkas apa saja yang sudah tidak digunakan dan menghapusnya jika tidak diperlukan			
Menghapus riwayat Wi-Fi pada ponsel agar tidak meninggalkan jejak digital			

TABEL PEMETAAN

Sensitivitas Data	Sebutkan data sensitif Anda dan sebutkan di mana saja dia berada			
Seberapa penting data berikut bagi anda Tinggi Sedang Rendah	Laptop Kerja 	Laptop Pribadi 	Ponsel Kerja 	Ponsel Pribadi 
Pesan (chat, media sosial)				
Pesan Surel				
Alamat Surel (donor, mitra, dll)				
Nomor telepon kontak				
Rekaman Video				
Foto				
Rekaman Audio				
Pesan Media Sosial				
Laporan Keuangan				
Nomor Rekening				
Credentials (username/ password)				
Informasi dan data program				
Laporan program				

Cloud Storage Lembaga 	Cloud Storage Personal 	SMS 	Surel Kerja 	Surel Pribadi 	HD Luar 	USB 




SAFEnet