2024

Kajian Ketahanan Siber

MANAJEMEN KERENTANAN

Sebuah Kolaborasi *Quad Helix* demi Ketahanan Siber Indonesia

HUAWEI

CDEF

KAJIAN KETAHANAN SIBER

MANAJEMEN KERENTANAN

Taufik Nurhidayat, S.ST dkk

TIM REDAKSI

TIM PENULIS

Taufik Nurhidayat, S.ST. (Ketua Tim Penulis)
Digit Oktavianto (Wakil Ketua)
Dr. Susila Windarta, S.Kom., M.Si.
Nanang Trianto, S.ST., M.AP.
Iqbal Firmansyah, M.T.
M. Fadhli Maghfur Shofiyuddin, M.Kom
Nabella Permatasari , S.Tr.Kom
Satrya Mahardhika, S.Tr.Kom
Muhammad Azza Ulin Nuha, S.Tr.Kom
Dwi Novazrianto, S.Tr.Kom
Alfian Adi Saputra, S.Tr.Kom

EDITOR DAN LAYOUT

Nur Annisa Kadarwati Febriyani, S.Tr.Kom

Cetakan pertama Januari 2025

Dirtebitkan oleh:
Politeknik Siber dan Sandi Negara Press

KATA PENGANTAR

Puji syukur kami panjatkan kepada Tuhan Yang Maha Esa atas berkat dan rahmat-Nya sehingga buku ini dapat diselesaikan. Dalam menghadapi era digital yang terus berkembang pesat, keamanan siber telah menjadi kebutuhan fundamental bagi setiap institusi, baik di sektor publik maupun swasta. Serangan siber yang semakin canggih dan kompleks memerlukan pendekatan manajemen kerentanan yang sistematis, inovatif, dan tangguh. Buku ini hadir untuk memberikan panduan komprehensif mengenai manajemen kerentanan, mulai dari konsep dasar hingga penerapan praktis di berbagai sektor, dengan harapan memberikan kontribusi nyata dalam memperkuat ketahanan siber nasional.

Dalam buku ini, pembaca akan menemukan pendekatan terkini dalam mengidentifikasi, menilai, dan menangani kerentanan yang ada di berbagai infrastruktur teknologi informasi. Kami menyajikan strategi-strategi efektif yang telah terbukti mampu menghadapi tantangan global yang terus berkembang. Lebih dari itu, kami menekankan pentingnya kolaborasi antara pemangku kepentingan, mulai dari peneliti, vendor, hingga regulator, dalam menciptakan ekosistem keamanan yang kuat. Manajemen kerentanan bukanlah sekadar respons terhadap ancaman, tetapi merupakan langkah proaktif yang harus terus ditingkatkan seiring dengan dinamika ancaman global.

Dengan penuh keyakinan, kami percaya bahwa buku ini akan menjadi rujukan penting bagi para profesional keamanan siber, akademisi, serta praktisi yang terlibat dalam pengelolaan dan perlindungan infrastruktur digital. Kami juga optimis bahwa panduan dan strategi yang disampaikan di dalamnya dapat memberikan solusi nyata bagi berbagai tantangan keamanan siber yang dihadapi Indonesia saat ini. Terima kasih kepada semua pihak yang telah berkontribusi dalam penyusunan buku ini. Kami percaya bahwa kolaborasi ini akan

semakin memperkuat ketahanan siber di Indonesia dan mengantarkan bangsa ini menuju keamanan digital yang lebih baik.

Selamat membaca!

Jangan pernah lelah mencintai Indonesia.

SAMBUTAN

Kepala Badan Siber dan Sandi Negara

Letjen TNI (Purn) Hinsa Siburian

Sesuai dengan amanat Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yaitu untuk melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa, dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi dan keadilan sosial, BSSN melalui Perpres Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara turut serta menjalankan amanat konstitusi dalam menjaga ruang siber nasional. Hal ini sejalan dengan apa yang disampaikan pada berbagai forum pidato kenegaraan maupun kegiatan internasional bahwa Keamanan Siber harus menjadi fokus perhatian kita bersama

Di dalam era digital yang terus berkembang, kita dihadapkan pada tantangan besar di ruang siber. Ancaman terhadap sistem informasi dan infrastruktur digital semakin meningkat seiring dengan berkembangnya penggunaan teknologi. Serangan siber yang berakibat pada kebocoran data kini menjadi masalah yang sering kita dengar, hal ini tidak hanya berkaitan dengan persoalan teknis, melainkan juga menyangkut keamanan nasional dan data pribadi masyarakat.

BSSN sebagai garda terdepan dalam menghadapi ancaman siber terus berusaha mengambil langkah-langkah strategis untuk memperkuat keamanan siber di Indonesia, salah satunya melalui penyusunan berbagai dokumen dan standar yang dapat diimplementasikan oleh para pemilik sistem elektronik.

Buku Kajian Manajemen Kerentanan ini saya nilai penting untuk berbagai pihak, mengidentifikasi dan mengelola kerentanan dalam sistem sebelum dimanfaatkan dan dieksploitasi oleh pihak tidak bertanggung jawab. Manajemen kerentanan bukan hanya tentang menemukan kerentanan dalam sistem, tetapi tentang membangun sistem yang tangguh dan responsif terhadap perkembangan teknologi dan perubahan ancaman siber yang dinamis.

Buku ini membahas secara mendalam mengenai kerangka kerja dan praktik terbaik dalam melakukan manajemen kerentanan. Kami berharap agar buku ini dapat menjadi panduan bagi para pemangku kepentingan, baik di sektor pemerintah, industri, maupun sektor lainnya dalam menghadapi ancaman siber yang semakin kompleks. Mengelola kerentanan dengan baik adalah investasi jangka panjang dalam menjaga staibilitas dan keberlanjutan operasional. Hal ini tidak hanya melindungi data, tetapi juga membangun kepercayaan publik, menciptakan keamanan digital yang lebih baik, dan memastikan ekosistem digital kita tetap aman terlindungi.

Keamanan siber adalah tanggung jawab kita bersama. Melalui kolaborasi, komitmen, dan penerapan manajemen kerentanan yang tepat, kita dapat melangkah maju bersama dalam menjaga keamanan siber di Indonesia.

Jakarta, Oktober 2024

Kepala Badan Siber dan Sandi Negara
Letjen TNI (Purn) Hinsa Siburian

SAMBUTAN

Deputi Bidang Operasi Keamanan Siber dan Sandi

Mayjen TNI Dominggus Pakel, S.Sos., M.M.S.I

Keamanan siber adalah pondasi krusial dalam menjaga stabilitas nasional dan melindungi kepentingan publik dari ancaman siber yang semakin kompleks. Sebagai Deputi Bidang Operasi Keamanan Siber dan Sandi pada Badan Siber dan Sandi Negara (BSSN), saya memahami pentingnya manajemen kerentanan yang efektif sebagai salah satu kunci utama dalam pengelolaan risiko siber organisasi. Buku Kajian Manajemen Kerentanan ini disusun untuk memberikan panduan yang terarah dan praktis bagi seluruh organisasi, khususnya Tim Tanggap Insiden Siber (TTIS) organisasi, dalam menghadapi ancaman siber yang terus berkembang.

Manajemen kerentanan adalah proses kritis yang tidak hanya melibatkan identifikasi dan mitigasi risiko secara teknis, tetapi juga perlu adanya kolaborasi antara berbagai pemangku kepentingan. Hal ini dikarenakan manajemen kerentanan adalah seni dalam memahami risiko dan menciptakan strategi pertahanan, dalam prosesnya, kolaborasi menjadi kunci untuk menghadapi ancaman yang ada. Harapannya, buku ini dapat memberikan wawasan mendalam tentang bagaimana mengelola kerentanan dengan pendekatan yang komprehensif dan adaptif serta kolaboratif antar pemangku kepentingan terkait.

Saya ucapkan terimakasih dan apresiasi yang tinggi kepada seluruh pihak yang terlibat dalam penyusunan buku ini, semoga buku kajian ketahanan siber terkait Manajemen Kerentanan ini dapat bermanfaat dalam meningkatkan ketahanan siber Indonesia.

Jakarta, Oktober 2024
Deputi Bidang Operasi Keamanan Siber dan Sandi

Mayjen TNI Dominggus Pakel, S.Sos., M.M.S.I

PRAKATA

Direktur Operasi Keamanan Siber

Andi Yusuf, M.T.

Salam sejahtera bagi kita bersama.
Mari kita menyampaikan rasa syukur kepada Tuhan Yang Maha Esa atas nikmat dan karunia-Nya sehingga buku dengan judul "Kajian Ketahanan Siber – Manajemen Kerentanan" dapat terselesaikan dengan baik. Kehadiran Direktorat Operasi Keamanan Siber menjadi bagian penting dalam pemberian dukungan penyusunan buku tentang pelaksanaan manajemen kerentanan di Indonesia sebagaimana sesuai dengan tugas dan fungsi sebagai pemberian dukungan pelaksanaan operasional keamanan siber.

Di tengah masifnya serangan siber yang terus meningkat, menjadi sangat penting untuk mengambil langkah-langkah antisipatif yang efektif. Manajemen kerentanan dalam buku ini bertujuan untuk memberikan panduan yang jelas dan praktis dalam mengelola kerentanan yang terdapat pada sistem elektronik dan menghadapi berbagai ancaman siber. Dengan pemahaman yang lebih baik tentang manajemen kerentanan, nantinya kita dapat meningkatkan kemampuan organisasi untuk mempersiapkan pengamanan lebih dini dan melindungi diri dari serangan yang semakin kompleks.

Ungkapan rasa terima kasih saya sampaikan kepada pihak-pihak yang telah berkontribusi dalam penyusunan buku ini. Semoga bisa mengambil banyak pembelajaran dan hikmah. Besar harapan saya semoga buku ini juga dapat bermanfaat bagi pembaca untuk menambah pengetahuan dan meningkatkan ketahanan dan keamanan siber di Indonesia.

Jakarta, Oktober 2024

Direktur Operasi Keamanan Siber
Andi Yusuf, M.T.

PRAKATA

Direktur Politeknik Siber dan Sandi Negara

Marsekal Pertama TNI
R. Tjahjo Khurniawan, S.T, M.Si

Dengan mengucap syukur kepada Tuhan Yang Maha Esa, saya merasa sangat bangga dapat memberikan prakata untuk buku ini, yang merupakan sebuah kontribusi berharga dalam mengembangkan wawasan dan pemahaman mengenai manajemen kerentanan di era digital. Sebagai institusi pendidikan yang berfokus pada pengembangan talenta di bidang keamanan siber dan persandian, Politeknik Siber dan Sandi Negara memiliki komitmen kuat untuk mencetak generasi profesional yang kompeten dan siap menghadapi tantangan siber yang semakin kompleks.

Keamanan siber bukan hanya tanggung jawab satu pihak, melainkan sebuah upaya kolektif yang melibatkan pemerintah, sektor swasta, dan masyarakat luas. Buku ini hadir sebagai panduan komprehensif yang akan sangat berguna bagi para praktisi, akademisi, dan profesional muda yang sedang meniti karier di dunia keamanan siber. Manajemen kerentanan, yang merupakan fokus utama dari buku ini, memberikan dasar kuat untuk memahami bagaimana ancaman dapat diidentifikasi, dimitigasi, dan dikelola secara proaktif, sebuah langkah penting dalam melindungi infrastruktur digital yang vital bagi keberlanjutan bangsa.

Sebagai lembaga pendidikan, Politeknik Siber dan Sandi Negara tidak hanya berfokus pada aspek teknis, tetapi juga pada pengembangan etika profesional dan kolaborasi lintas disiplin, yang semua itu tercermin dalam materi yang disampaikan dalam buku ini. Buku ini juga menjadi sarana untuk memperkuat kerja sama antara dunia akademik dan industri dalam menciptakan solusi inovatif yang dapat menghadapi ancaman siber secara efektif dan berkelanjutan.

Saya mengucapkan terima kasih kepada seluruh pihak yang telah berperan dalam penyusunan buku ini, mulai dari tim penulis hingga para kontributor ahli yang memberikan wawasan mereka. Dengan penuh keyakinan, saya percaya bahwa buku ini akan menjadi sumber referensi penting bagi para mahasiswa, dosen, serta para praktisi di bidang keamanan siber. Semoga buku ini dapat memberikan manfaat besar dan menjadi inspirasi bagi kita semua dalam menjaga dan memperkuat kedaulatan siber Indonesia.

Jakarta, Oktober 2024

Direktur Politeknik Siber dan Sandi Negara
Marsekal Pertama TNI R. Tjahjo Khurniawan, S.T, M.Si

RINGKASAN EKSEKUTIF

Tren serangan siber kian hari kian meningkat, tentunya hal ini menimbulkan risiko yang lebih besar terhadap kerentanan pada sistem elektronik. Organisasi perlu menjalankan tindakan proaktif dalam mengelola kerentanan, diawali dengan identifikasi kerentanan, prioritisasi, penanganan, verifikasi dan evaluasi. Sehingga dapat meminimalisasi risiko kerentanan tersebut dieskploitasi oleh pihak yang tidak berwenang.

Dalam menjalankan siklus manajemen kerentanan di tingkat organisasi, Tim Tanggap Insiden Siber (TTIS) organisasi ataupun unit yang bertanggung jawab akan keamanan siber memiliki peran penting untuk memastikan bahwa setiap tahapan mulai dari identifikasi hingga evaluasi kerentanan berjalan dengan baik. Diperlukan adanya mekanisme untuk menerima laporan identifikasi kerentanan dari pihak internal maupun eksternal organisasi. Selanjutnya, kerentanan diukur dan ditangani untuk meremediasi kerentanan sebelum dieksploitasi oleh pihak lain.

Buku ini membahas secara mendalam terkait penerapan siklus manajemen kerentanan. Terdapat 2 jenis pendekatan, yakni studi literatur dan juga penerapan praktik terbaik terkait manajemen kerentanan. Proses studi literatur dilakukan dengan mendalami berbagai referensi, sementara penerapan praktik terbaik dipelajari dari penerapan manajemen kerentanan pada berbagai negara dan organisasi. Selain itu, juga dijelaskan strategi penerapan manajemen kerentanan pada organisasi dari sudut pandang TTIS.

Di sisi lain, manajemen kerentanan yang efektif dan efisien perlu diwujudkan lewat kolaborasi antara pihak terkait, khususnya pada level nasional. Buku ini juga mengkaji kerangka kerja manajemen kerentanan yang dapat diterapkan di Indonesia. Termasuk berbagai pihak yang

terkait serta peran dan tanggung jawabnya dalam kolaborasi Manajemen Kerentanan di Indonesia.

Melalui buku ini, diharapkan dapat menjadi langkah awal terwujudnya kolaborasi antara entitas terkait untuk menjalankan Manajemen Kerentanan yang terintegrasi dalam skala nasional. Dengan pembagian peran yang jelas dan tanggung jawab yang terukur, setiap entitas diharapkan dapat berkontribusi secara signifikan dalam mencegah dan menangani kerentanan, sehingga dapat meningkatkan ketahanan siber di Indonesia secara menyeluruh dan berkelanjutan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PERAN BSSN DALAM KEAMANAN RUANG SIBER

Keamanan siber bukan lagi pilihan, melainkan kebutuhan bagi setiap individu, bisnis, dan pemerintah. Karena ancaman siber tidak memandang siapa targetnya

- Hinsa Siburian, Kepala Badan Siber dan Sandi Negara -

A. Lanskap Keamanan Siber Indonesia

Lanskap Keamanan Siber Indonesia adalah persembahan Badan Siber dan Sandi Negara (BSSN). Sebuah laporan berkesinambungan kondisi Keamanan Siber Indonesia, pantauan 24 perhari, 7 hari dalam seminggu yang dikemas dalam laporan perbulan, dijadikan laporan tahunan sejak tahun 2020 hingga sekarang.

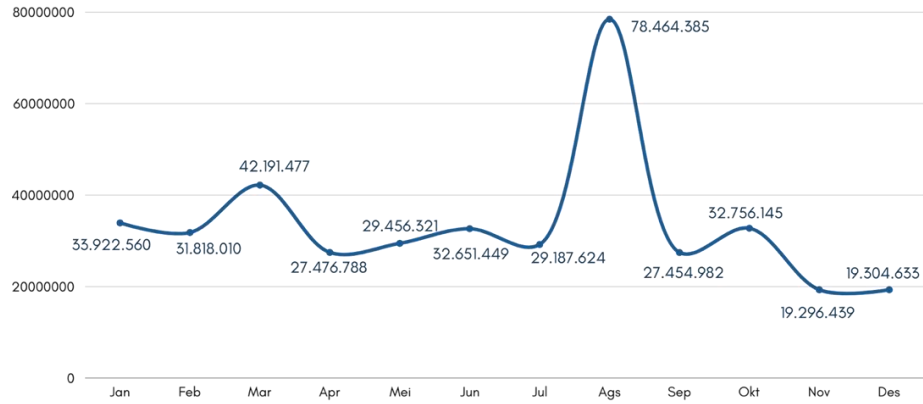
Lanskap keamanan Siber Indonesia berisi Laporan pemantauan trafik internet nasional, Kumpulan arikel tentang peringatan dini ancaman keamanan dan kerentanan sistem, Kumpulan berita tentang keamanan siber atau IT. Informasi ini menjadi dasar yang penting untuk menentukan kebijakan strategis negara dan memberikan panduan bagi masyarakat dalam beraktivitas di ruang siber. BSSN mengajak seluruh elemen masyarakat untuk terus berkolaborasi dan bersinergi dalam menjaga integritas ruang siber nasional dari berbagai ancaman siber.

Tahun 2024. Badan Siber dan Sandi Negara telah menerbitkan Lanskap Keamanan Siber Indonesia 2023 pada tanggal 4 Maret 2024. Lanskap ini merupakan kajian strategis yang disusun berdasarkan hasil pemantauan trafik keamanan siber selama 24 jam sehari, 7 hari seminggu, sepanjang tahun 2023 oleh Direktorat Operasi Keamanan Siber BSSN. Lanskap Keamanan Siber memberikan gambaran mengenai kondisi dunia siber di Indonesia selama tahun 2023 dan menjadi acuan untuk menyusun strategi keamanan siber tahun 2024. Berdasarkan hasil pemantauan tersebut, tercatat ada total 403.990.813 anomali, 4.001.905 aktivitas *Advanced Persistent Threat* (APT), dan 1.011.209 aktivitas *ransomware* (Direktorat Operasi Keamanan Siber, 2023). Beberapa hasil yang dilaporkan yaitu:

1. Anomali Trafik

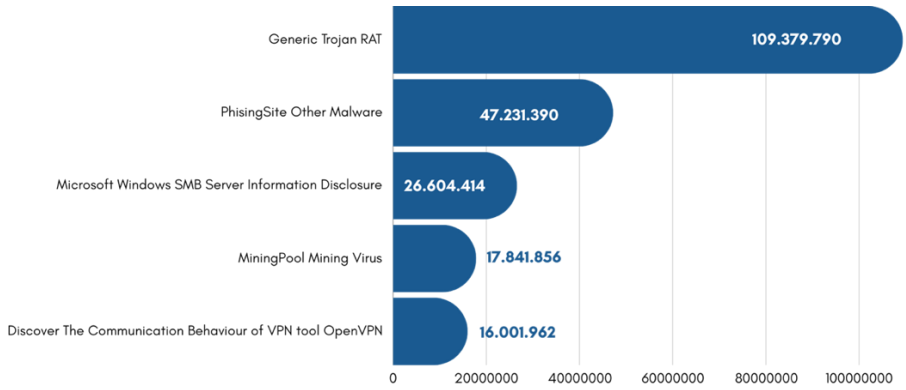
Aktivitas anomali trafik dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi. Anomali trafik tertinggi terjadi pada bulan Agustus sejumlah 78.464.385

dan terendah pada bulan November sejumlah 19.296.439 sebagaimana tercantum pada Gambar 1. Berdasarkan sumber anomali trafik tersebut, terdapat 5 negara yang merupakan sumber anomali trafik terbesar yaitu Indonesia, Amerika Serikat, Singapura, Jerman dan Belanda. Sedangkan lima negara tujuan anomali terbesar adalah Indonesia, Amerika Serikat, Jerman, Belanda dan Prancis sebagaimana dicantumkan dalam Gambar 2.



Gambar 1. Grafik Anomali Trafik

Gambar 2. Negara terbesar sumber dan tujuan anomali



Gambar 3. Top 5 Anomali Trafik

Pantauan anomali trafik disebabkan oleh beberapa aktivitas serangan siber dengan frekuensi tertinggi. Lima aktivitas serangan siber dengan frekuensi tertinggi disajikan pada Gambar 3 yaitu *Generic Trojan* RAT, *PhishingSite Other Malware*, *Microsoft Windows SMB Server Information Disclosure*, *MiningPool Mining Virus*, serta *Discover the Communication Behavior of VPN Tool OpenVPN*.

Aktivitas Generic Trojan RAT bersumber dari terdeteksinya *signature* yang timbul akibat adanya aktivitas *backdoor communication* menuju domain *malicious* yang terindikasi sebagai *command and control* server milik *threat actor*. Munculnya aktivitas ini dapat berakibat pada indikasi pencurian informasi, penghapusan data, pemblokiran, penyalinan informasi, serta menjalankan program pada perangkat yang terinfeksi di luar kehendak pengguna (Direktorat Operasi Keamanan Siber, 2023).

Aktivitas selanjutnya yang masif adalah *Phishing Site Other Malware*. *Phishing Site* merupakan situs palsu untuk menipu pengguna supaya memberikan informasi pribadi seperti, *password,* nomor kependudukan, dan rincian keuangan maupun data pribadi lainnya. Sedangkan *malware* merupakan kode jahat yang memiliki tujuan untuk merusak atau menganggu kinerja suatu perangkat maupun sistem. Jadi,

phishing site Other Malware merupakan *malware* yang memanfaatkan situs *phishing* untuk menginfeksi korbannya.

Peringkat ketiga penyumbang aktivitas anomali terbanyak adalah *microsoft windows smb server information disclosure* yang terdeteksi karena adanya protokol SMBv1 yang sudah usang sehingga dapat dimanfaatkan penyerang untuk memperoleh informasi sensitif. SMB merupakan protokol yang digunakan untuk berbagi *file*, mencetak *file* dan komunikasi antar perangkat dalam suatu jaringan (Direktorat Operasi Keamanan Siber, 2023). Selain itu, kerentanan ini juga dapat dimanfaatkan penyerang untuk menginjeksi *malware* seperti *WannaCry, Trickbot, CoinMiner*, dan *WannaMine* ke dalam sistem.

Posisi keempat aktivitas anomali terbanyak adalah *miningpool mining virus* atau yang lebih dikenal dengan *crypto mining malware*. Seperti namanya, aktivitas ini merupakan *malware* yang menggunakan sumber daya komputer korban untuk melakukan penambangan mata uang kripto. Perangkat korban bisa mengalami penurunan kinerja bahkan bisa rusak akibat dari aktivitas *malware* ini.

Aktivitas terbanyak kelima dari keseluruhan anomali yaitu *discover the communication behavior of vpn tool openvpn*. Aktivitas ini terdeteksi akibat adanya penggunaan VPN dengan aplikasi OpenVPN. Protokol VPN digunakan untuk membuat koneksi internet dengan menggunakan *point to point* (PTP) yang telah dienkripsi dengan *username* dan *password* (Direktorat Operasi Keamanan Siber, 2023). Aplikasi OpenVPN sebenarnya legal, namun saat ini banyak penyerang yang memanfaatkannya untuk melakukan spionase pada perangkat pengguna dengan menyisipkan *malware* di dalamnya.

2. Advanced Persistent Threat (APT)

Berdasarkan hasil pengamatan Direktorat Operasi Keamanan Siber BSSN, aktivitas APT di Indonesia terdeteksi sebanyak 4.001.905 sepanjang tahun 2023 (Direktorat Operasi Keamanan Siber, 2023). APT merupakan istilah untuk menggambarkan sebuah organisasi atau

sekelompok orang untuk melakukan serangan siber kepada sistem tertentu dengan tujuan untuk mengambil keuntungan seperti spionase, pencurian uang, pencurian data dan sebagainya. APT melakukan serangan dengan menggunakan teknik yang canggih sehingga dapat bertahan lama tanpa terdeteksi oleh perangkat keamanan pada sistem korban. Gambar 4 menyajikan informasi terkait lima APT yang paling banyak ditemukan di ruang siber Indonesia.

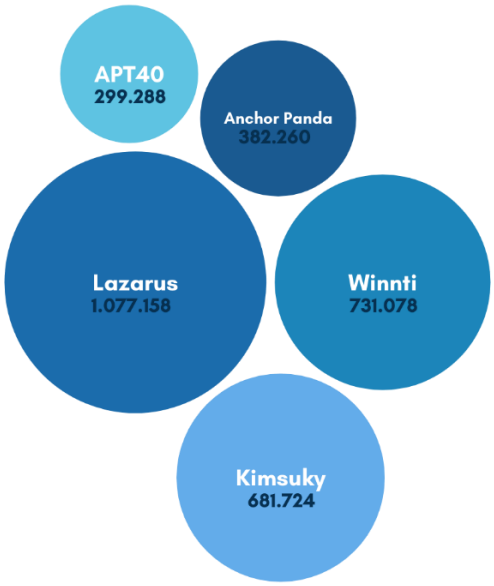
Gambar 4. Top 5 APT

3. Ransomware

Ransomware adalah jenis *malware* yang mengenkripsi data atau perangkat korban, kemudian meminta bayaran sebagai syarat untuk memperoleh kunci dekripsi. Serangan ini dapat mengakibatkan berbagai kerugian, seperti kehilangan data penting, kehilangan akses ke aset digital yang terinfeksi, dan kerugian finansial yang signifikan, terutama bagi organisasi dan perusahaan yang terganggu operasionalnya. Selain itu, serangan *ransomware* dapat menimbulkan biaya tambahan, seperti biaya pemulihan sistem dan peningkatan keamanan untuk mencegah serangan serupa di masa depan.

Ransomware tidak hanya menyerang perusahaan besar atau organisasi, tetapi juga individu dan bisnis kecil. Hal ini menunjukkan bahwa serangan *ransomware* bersifat acak dan dapat menargetkan siapa saja yang memiliki celah keamanan. Lima jenis *ransomware* yang paling aktif pada tahun 2023 yaitu *Luna Moth, WannaCry, Locky, LockBit*, dan *Grandcrab*. Jenis-jenis *ransomware* ini dikenal karena penyebaran yang luas dan dampak destruktif pada berbagai sektor. Jumlah serangan dan

detail lain terkait *ransomware* ini disajikan pada Gambar 5 (Direktorat Operasi Keamanan Siber, 2023).



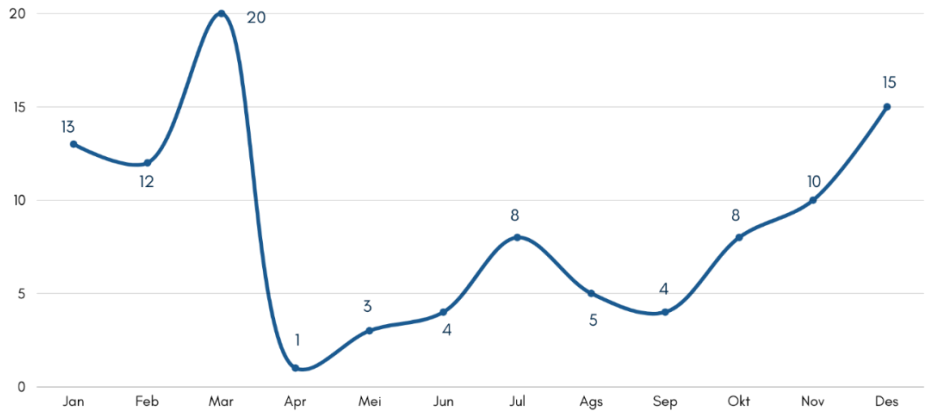
Gambar 5. Top 5 Ransomware

4. Web Defacement

Web defacement merupakan jenis serangan yang memanfaatkan kerentanan pada aplikasi *web* dengan mengubah tampilan, bahkan dalam beberapa kasus menghapus konten dari situs *web* yang berhasil dieksploitasi. Serangan ini biasanya bertujuan untuk merusak reputasi atau menyebarkan pesan tertentu melalui situs *web* yang telah disusupi. Terdapat total 189 kasus yang telah diberikan notifikasi kepada pemilik sistem (Direktorat Operasi Keamanan Siber, 2023). Sektor yang paling tinggi mengalami *web defacement* adalah sektor Administrasi Pemerintahan dengan 167 kasus, kemudian kasus lain terdapat pada sektor kesehatan sebanyak 7 kasus, sektor pertahanan 3 kasus dan 12 kasus pada sektor lainnya.

5. Data breach

Data breach atau kebocoran data merupakan serangan siber dengan cara mengambil data sensitif dari aset pengguna lalu diekspos atau diperjual belikan. Penyerang dapat memperoleh data sensitif dari aset dengan memanfaatkan kerentanan pada sistem kemudian melakukan eksploitasi. Selama tahun 2023, BSSN mendeteksi adanya 103 dugaan insiden kebocoran data (Direktorat Operasi Keamanan Siber, 2023). Kasus terbanyak terjadi pada bulan Maret sebanyak 20 kasus, sedangkan kasus paling sedikit ada pada bulan April sebanyak 1 kasus. Rincian kasus setiap bulan dapat dilihat pada Gambar 6.



Gambar 6. Kasus Kebocoran Data per bulan pada 2023

6. Common Vulnerabilities and Exposures (CVE)

CVE adalah daftar kerentanan yang diakui secara global dan digunakan untuk berbagi informasi terkait kerentanan aset. Setiap entri CVE mencakup nomor identifikasi, deskripsi kerentanan, serta dampak yang ditimbulkan. Selama tahun 2023, BSSN telah menerbitkan 66 imbauan keamanan. Sistem untuk mengukur dan mengategorikan tingkat keparahan kerentanan menggunakan *Common Vulnerability Scoring System* (CVSS). Dari seluruh imbauan tersebut, terdapat 5 CVE

yang memiliki potensi dampak terbesar di Indonesia sepanjang tahun 2023 (Direktorat Operasi Keamanan Siber, 2023). Kelima CVE tersebut yaitu CVE-2022-22721, CVE-2022-26377, CVE-2023-0662, CVE-2023-30799, dan CVE-2022-3602 dengan penjelasan sebagai berikut:

a) CVE-2022-22721 (*Apache* HTTP *Server buffer overflow)*

CVE-2022-22721 terjadi ketika *LimitXMLRequestBody* pada *Apache* HTTP *Server* sistem 32bit versi 2.4.52 atau sebelumnya mengizinkan permintaan *(request body)* lebih besar dari 350MB. Sedangkan kemampuan sebenarnya hanya mampu menampung permintaan sebesar 1 MB, sehingga kesalahan pengaturan tersebut dapat mengakibatkan terjadinya *buffer overflow*[1].

Dampak dari *buffer overflow* dapat mengganggu aspek ketersediaan layanan pada sistem bahkan bisa menjadi celah penyerang untuk melakukan serangan lanjutan seperti *arbitrary code execution*[2]. Hasil nilai CVSS dari CVE-2022-22721 adalah 9,1 dengan kategori dampak *critical* (Direktorat Operasi Keamanan Siber, 2023).

b) CVE-2022-26377 (HTTP *request smuggling)*

CVE-2022-26377 memiliki nilai CVSS sebesar 7,5 dengan tingkat dampak *high* (Direktorat Operasi Keamanan Siber, 2023). Kerentanan CVE-2022-26377 terjadi ketika terdapat kerentanan inkonsisten interpretasi dari permintaan HTTP (HTTP *request smuggling*) dalam *mod_proxy_ajp* dari Apache HTTP *Server* yang mengizinkan penyerang untuk melakukan penyelundupan permintaan ke Apache JServ Protocol (AJP) *server*[3]. HTTP *request smuggling* merupakan sebuah teknik yang digunakan penyerang dengan menyisipkan dua *request* atau lebih dalam satu kali pengiriman HTTP untuk mengelabuhi server[4]. Dengan memanfaatkan CVE-2022-26377 *threat actor* dapat menyisipkan permintaan yang akan merugikan sistem, baik menghapus, merubah

[1] https://nvd.nist.gov/vuln/detail/CVE-2022-22721

[2] https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

[3] https://nvd.nist.gov/vuln/detail/CVE-2022-26377

[4] https://kamsib.id/penetration-testing/http-request-smuggling-kerentanan-unik-dari-http-1-1/

maupun memodifikasi data. Perangkat yang rentan yaitu Apache HTTP *Server* versi 2.4.53 dan sebelumnya.

c) CVE-2023-0662 (*denial of servise on* PHP)

CVE-2023-0662 terjadi karena konfigurasi *default* PHP pada proses *parsing multipart request body* yang mengizinkan akses ke CPU *time* dalam jumlah besar tanpa autentikasi sehingga dapat menimbulkan serangan *denial of service*[5]. Serangan *denial of service* dilakukan dengan cara mengirimkan *request* dalam jumlah besar ke sistem sehingga menimbulkan *excessive logging* (pencatatan yang berlebihan) yang dapat mengganggu ketersediaan sistem korban. CVE-2023-0662 memiliki nilai CVSS 7,5 dengan tingkat dampak *high*, dan sistem yang terdampak adalah PHP 8.0 (sebelum versi 8.0.28), PHP 8.1 (sebelum versi 8.1.16), PHP 8.2 (sebelum versi 8.2.3) (Direktorat Operasi Keamanan Siber, 2023).

d) CVE-2023-30799 (Privilege escalation on MikroTik RouterOS)

CVE-2023-30799 terjadi pada MikroTik RouterOS *stable* pada versi sebelum 6.49.7 dan *long-term* 6.48.6 yang memiliki kerentanan *privilege escalation* karena pengguna bisa meningkatkan kewenangan dari admin menjadi super-admin melalui Winbox atau HTTP[6]. CVE ini memiliki nilai CVSS 7,2 dengan dampak *high* (Direktorat Operasi Keamanan Siber, 2023).

e) CVE-2022-3602

CVE-2022-3602 merupakan kerentanan yang terjadi pada Open SSL 3.0 ketika proses verifikasi sertifikat, mengharuskan *Certificate Authority* (CA) menandatangani sertifikat walaupun gagal membuat jalur *trusted issuer*[7]. CVE ini berpotensi berbahaya karena memungkinkan aplikasi melanjutkan verifikasi pada sertifikat yang tidak dipercaya. CVE-2022-3602 memiliki nilai CVSS 7,5 dengan tingkat dampak *high*.

[5] https://nvd.nist.gov/vuln/detail/CVE-2023-0662

[6] https://nvd.nist.gov/vuln/detail/CVE-2023-30799

[7] https://nvd.nist.gov/vuln/detail/CVE-2022-3602

B. Tren Kerentanan Sistem Elektronik Instansi Pemerintah Di Indonesia

Berdasarkan Keputusan Kepala BSSN Nomor 293 Tahun 2023 tentang Pelayanan Publik, BSSN memiliki 9 macam layanan salah satunya adalah layanan *Information Technology Security Assessment* (ITSA). ITSA merupakan kegiatan pengujian terhadap keamanan sistem elektronik untuk mengidentifikasi dan mengevaluasi potensi risiko keamanan informasi serta memberikan rekomendasi berdasarkan temuan kerentanan. Selama tahun 2023 BSSN telah melaksanakan kegiatan ITSA pada 138 instansi dengan jumlah 586 sistem elektronik yang telah diuji dan temuan sebanyak 2.860. Sistem elektronik yang diuji meliputi aplikasi *web*, *mobile* dan infrastruktur. Kerentanan yang ditemukan dibagi menjadi beberapa kategori berdasarkan tingkat risiko yaitu *critical, high, medium, low* dan *info*. Dari 2.860 kerentanan, terdapat 418 kerentanan kategori *critical,* 533 kerentanan kategori *high*, 486 kerentanan kategori *medium*, 846 kerentanan kategori *low* dan 577 katagori *info*. Berdasarkan seluruh kerentanan yang terdeteksi, berikut 5 (lima) kerentanan dengan tingkat risiko *critical* (Direktorat Operasi Keamanan Siber, 2023):

1. *Insecure Direct Object Reference* (IDOR)

IDOR merupakan kerentanan yang muncul ketika penyerang dapat mengakses atau memodifikasi objek dengan memanipulasi parameter pada URL *web*, karena tidak adanya pemeriksaan atau verifikasi pengguna dalam proses akses[8]. Untuk mengatasi kerentanan IDOR, sistem harus menerapkan kontrol akses yang ketat, menerapkan

[8] https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

verifikasi pengguna dan menggunakan enkripsi pada parameter supaya tidak mudah ditebak.

2. *Broken Access Control* (BAC)

Broken Access Control merupakan kerentanan urutan pertama dalam OWASP Top 10 dengan kode A01:2021-Broken Access Control (OWASP Foundation, 2021) yang terjadi ketika pengguna dapat melakukan akses, memodifikasi atau merusak seluruh data di luar izin kewenangannya[9]. Kerentanan ini dapat menjadi celah penyerang untuk mendapatkan akses yang tidak sah dari suatu aplikasi. BAC dapat dicegah dengan menerapkan kebijakan akses yang ketat, pada sisi *client* maupun *server*.

3. SQL *Injection*

SQL *Injection* merupakan jenis serangan injeksi yang memungkinkan penyerang melakukan *input* kode eksploit tertentu sehingga dapat melakukan *bypass* untuk mendapatkan akses langsung ke basis data aplikasi[10]. Serangan ini menjadi salah satu teknik dalam insiden *data breach*. Setelah penyerang mendapatkan akses basis data dan terdapat informasi *critical* maka penyerang dapat memperjual belikan data tersebut. Untuk mencegah terjadinya SQL *Injection* adalah menerapkan sanitasi dan validasi *input* pada semua *form input* aplikasi dan melakukan *update* aplikasi basis data secara berkala.

4. *File Upload Vulnerability*

File Upload Vulnerability terjadi ketika sebuah *web server* mengizinkan pengguna untuk mengunggah *file* ke dalam sistem tanpa adanya validasi nama, jenis, isi maupun ukuran dari *file*[11]. Kerentanan ini dapat dimanfaatkan oleh penyerang dengan mengunggah *file* php atau jsp untuk mendapatkan *web shell* dalam aplikasi. Untuk mengatasi *file upload vulnerability* penting untuk melakukan validasi ketat terhadap jenis dan ekstensi *file* yang diunggah, serta memeriksa keabsahan file

[9] https://owasp.org/Top10/A01_2021-Broken_Access_Control/

[10] https://owasp.org/www-community/attacks/SQL_Injection

[11] https://portswigger.net/web-security/file-upload

sebelum melakukan eksekusi (Direktorat Operasi Keamanan Siber, 2023).

5. *Privilege Escalation*

Privilege escalation merupakan serangan yang dilakukan untuk mendapatkan akses yang tidak sah ke dalam sistem[12]. Serangan ini dapat berdampak pada pengambil alihan akun, kehilangan data, bahkan kerusakan sistem karena ketika penyerang mendapatkan kewenangan yang tinggi, dapat melakukan apa pun di luar perkiraan korban. Untuk menghindari serangan *privilege escalation* harus menerapkan prinsip pemisahan hak istimewa dan melakukan pembatasan akses yang ketat terhadap setiap *role* pengguna.

C. Urgensi Manajemen Kerentanan di Indonesia

Data lanskap keamanan siber 2023 menunjukkan terdapat ancaman siber yang serius pada sistem elektronik di Indonesia. Indonesia mengalami peningkatan signifikan dalam jumlah dan kompleksitas serangan siber, khususnya terhadap instansi pemerintah dan infrastruktur kritis. Sedangkan data kerentanan yang ditemukan pada instansi Pemerintah memberikan informasi bahwa masih terdapat banyak celah kerentanan yang bersifat kritikal pada sistem elektronik instansi pemerintahan di Indonesia. Celah keamanan tersebut dapat berdampak buruk apabila tidak ditutup atau ditangani dengan baik. Berdasarkan kondisi tersebut, melakukan pengelolaan atau manajemen terhadap kerentanan-kerentanan yang ditemukan menjadi salah satu aspek yang penting. Selain itu, terdapat beberapa alasan yang mendasari mengapa manajemen kerentanan menjadi prioritas yang mendesak sebagai berikut:

1. Peningkatan Serangan Siber dan Target Sektor Pemerintah.

[12] https://www.crowdstrike.com/cybersecurity-101/privilege-escalation/

Tren serangan siber yang terus meningkat menunjukkan bahwa sistem elektronik pemerintah yang mengelola data dan informasi penting masih rentan terhadap eksploitasi celah keamanan.

2. Kerentanan pada Infrastruktur Kritis dan Sistem Elektronik.
   Sistem elektronik pemerintah sering kali memiliki kerentanan pada aplikasi *web*, jaringan, dan perangkat lunak yang tidak diperbarui. Kerentanan bersifat *zero-day* juga menjadi ancaman serius karena eksploitasi kelemahan ini sering terjadi sebelum adanya pembaruan keamanan dari pengembang. Selain itu, infrastruktur kritis seperti sistem komunikasi, transportasi, dan pelayanan publik dapat mengalami gangguan signifikan jika tidak terdapat strategi manajemen kerentanan yang baik.
3. Dampak Kerusakan Ekonomi dan Keamanan Nasional.
   Serangan terhadap sistem elektronik pemerintah dapat berdampak pada layanan publik, menyebabkan kerugian ekonomi, dan menurunkan tingkat kepercayaan masyarakat terhadap pemerintah. Sebagai contoh adalah kasus pencurian data sensitif dapat memicu tindak lanjut berupa penipuan identitas dan pelanggaran privasi yang merugikan banyak pihak. Di sisi lain, ketidakamanan siber juga dapat berdampak pada stabilitas keamanan nasional, mengingat adanya ancaman dari kelompok peretas (*hacktivist*) yang menargetkan institusi pemerintah dan infrastruktur penting negara.
4. Kewajiban Regulasi dan Penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE).
   Dengan diterapkannya SPBE, instansi pemerintah diharuskan untuk menerapkan sistem elektronik yang terintegrasi dan aman. Hal ini mendorong perlunya manajemen kerentanan yang baik agar sistem yang digunakan sesuai dengan standar keamanan yang diharapkan. Beberapa regulasi seperti UU ITE juga mengamanatkan bahwa setiap instansi wajib menjaga keamanan data dan sistem informasi yang dikelola, sehingga upaya manajemen kerentanan menjadi bagian dari pemenuhan kewajiban hukum.
5. Kurangnya Sumber Daya dan Kompetensi Keamanan Siber.

Masih terdapat instansi pemerintah daerah yang kekurangan sumber daya manusia dan kapabilitas teknis untuk mengidentifikasi, mengevaluasi, dan mengelola kerentanan dengan baik. Hal ini menyebabkan adanya celah keamanan yang dapat dieksploitasi oleh penyerang. Oleh karena itu, program pelatihan dan peningkatan kompetensi di bidang keamanan siber masih menjadi kebutuhan utama untuk memastikan kesiapan sumber daya manusia dalam menghadapi ancaman siber.

Dari beberapa alasan yang telah dijabarkan sebelumnya, urgensi manajemen kerentanan di Indonesia berfokus pada peningkatan kesiapan, mitigasi risiko, dan pencegahan terhadap ancaman siber yang semakin meningkat, serta memastikan bahwa sistem elektronik yang digunakan oleh pemerintah mampu beroperasi secara aman dan andal.

BAB II
REGULASI KEAMANAN SISTEM ELEKTRONIK

There are two types of companies: those that have been hacked, and those who don't know they have been hacked

- John Chambers

Praktisi dan profesional yang menggeluti ruang siber untuk pribadi, organisasi atau perusahaan agar nyamandan aman dalam bekerja, sebaiknya mengetahui kebijakan dan beberapa aspek legalitas yang berkaitan dengan aktivitas menjaga ruang siber. Mari kita telaah dan memahami regulasi serta kebijakan yang menjadi dasar hukum.

Manajemen kerentanan dalam keamanan siber merupakan elemen krusial untuk menjaga integritas, ketersediaan, dan kerahasiaan sistem informasi di era digital yang semakin berkembang pesat. Seiring dengan peningkatan jumlah serangan siber dan kompleksitas ancaman yang dihadapi oleh organisasi, pendekatan yang sistematis dan terstruktur sangat dibutuhkan untuk mengidentifikasi, menilai, dan mengelola kerentanan yang dapat dieksploitasi. Dalam konteks ini, kerangka regulasi yang komprehensif, seperti yang diatur dalam berbagai undang-undang dan peraturan di Indonesia, berperan penting dalam membentuk landasan hukum serta pedoman bagi organisasi dalam memperkuat keamanan siber dan mengurangi risiko yang terkait dengan transaksi elektronik dan infrastruktur digital.

Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), yang pertama kali disahkan melalui UU No. 11 Tahun 2008 dan mengalami sejumlah perubahan dengan UU No. 19 Tahun 2016 serta UU No. 1 Tahun 2024, menjadi dasar hukum utama dalam pengelolaan informasi digital, perlindungan data, serta mitigasi kerentanan pada transaksi elektronik. UU ini menekankan pentingnya perlindungan sistem elektronik dari segala bentuk penyalahgunaan serta penegakan hukum yang kuat terhadap aktivitas yang mengancam keamanan digital. Dalam konteks tersebut, UU ITE menyoroti urgensi keamanan siber di tengah laju perkembangan teknologi dan meningkatnya volume transaksi digital di Indonesia.

Peraturan Pemerintah No. 71 Tahun 2019, yang mengatur tata cara penyelenggaraan sistem dan transaksi elektronik, menetapkan kewajiban bagi instansi pemerintah dan sektor publik untuk menerapkan langkah-langkah keamanan yang sesuai. Peraturan ini mengharuskan

adanya pengelolaan risiko yang menyeluruh, termasuk mitigasi kerentanan dalam infrastruktur digital yang digunakan oleh pemerintah. PP ini menjadi fondasi penting bagi penerapan tata kelola keamanan informasi yang baik dalam menghadapi risiko dari adopsi teknologi digital dalam administrasi publik.

Peraturan Presiden No. 82 Tahun 2022 dan No. 47 Tahun 2023 memperkuat perlindungan terhadap Infrastruktur Informasi Vital (IIV) serta menetapkan Strategi Keamanan Siber Nasional. Kedua peraturan ini mencakup pengelolaan kerentanan siber, mitigasi risiko, dan pengembangan respons terhadap krisis siber yang dapat mengancam infrastruktur penting negara. Melalui regulasi ini, pemerintah menegaskan komitmen mereka dalam melindungi infrastruktur strategis negara dari ancaman siber yang semakin kompleks.

Di sektor pemerintahan, Peraturan Menteri PANRB No. 5 Tahun 2020 dan Peraturan Badan Siber dan Sandi Negara (BSSN) No. 4 Tahun 2021 memberikan pedoman rinci terkait manajemen risiko dan keamanan informasi pada sistem pemerintahan berbasis elektronik (SPBE). Regulasi ini membantu pemerintah dalam mengidentifikasi, mengelola, serta mengurangi kerentanan yang dapat membahayakan infrastruktur digital pemerintahan, sehingga memperkuat keseluruhan sistem keamanan siber di sektor publik.

Selain itu, Peraturan BSSN Nomor 7, 8, 9, dan 10 Tahun 2023 serta No. 5 Tahun 2024, membentuk kerangka kerja yang lebih terstruktur untuk mengidentifikasi dan meningkatkan keamanan infrastruktur informasi vital. Regulasi ini juga mengatur pengukuran tingkat kematangan keamanan siber, peningkatan kompetensi sumber daya manusia, serta perencanaan aksi nasional dalam menghadapi ancaman siber. Lebih lanjut, Peraturan Deputi III No. 1 Tahun 2024 memperkuat pembentukan TTIS di sektor pemerintahan untuk meningkatkan respons cepat terhadap insiden siber dan pengelolaan kerentanan secara efektif. Seluruh regulasi ini mencerminkan pendekatan komprehensif pemerintah dalam mengelola risiko siber, memperkuat infrastruktur digital, serta melindungi keamanan nasional.

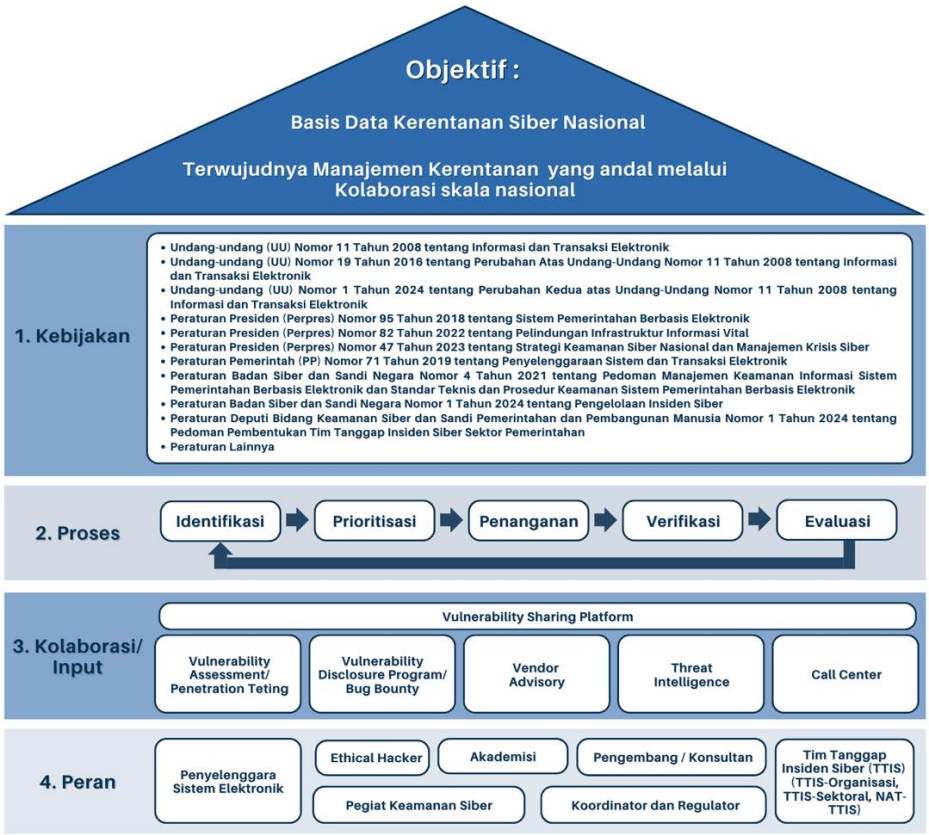
BAB III
KERANGKA KERJA MANAJEMEN KERENTANAN DI INDONESIA

You can't protect what you don't understand.

- Gerald Friedland

A. Kerangka Kerja Manajemen Kerentanan di Indonesia

Dalam rangka penerapan manajemen kerentanan di Indonesia, pada bagian ini dijelaskan desain kerangka kerja yang dapat diterapkan di Indonesia dengan menggambarkan dasar kebijakan yang menjadi rujukan, proses manajemen kerentanan, kolaborasi/input dari kerentanan, hingga entitas-entitas yang terlibat dalam proses manajemen kerentanan.



Gambar 7. Kerangka kerja Manajemen Kerentanan Indonesia

Gambar 7 mengilustrasikan kerangka kerja strategis dalam penerapan manajemen kerentanan di Indonesia. Tujuan utama dari

kerangka kerja ini adalah membangun basis data kerentanan nasional serta mewujudkan manajemen kerentanan yang andal melalui kolaborasi skala nasional.

Bagian pertama dari kerangka kerja adalah landasan hukum dan peraturan yang mendasari penyusunan dan pelaksanaan manajemen kerentanan. Bagian ini mencakup Undang-Undang, Peraturan Presiden, Peraturan Pemerintah, Peraturan Badan Siber dan Sandi Negara, dan Peraturan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia. Landasan hukum yang dipilih dan digunakan pada kerangka kerja manajemen kerentanan tersebut merupakan peraturan terkait informasi dan transaksi elektronik, sistem pemerintahan berbasis elektronik, strategi keamanan siber nasional dan manajemen krisis siber, serta pengaturan mengenai TTIS.

Bagian kedua dari kerangka kerja manajemen kerentanan adalah siklus manajemen kerentanan. Siklus ini terdiri dari tahap identifikasi hingga penanganan terhadap kerentanan yang ditemukan. Tahapan yang harus dilalui dalam siklus manajemen kerentanan adalah mengidentifikasi aset, mengidentifikasi kerentanan melalui proses pengujian atau berdasarkan laporan kerentanan, melakukan validasi dan penilaian risiko untuk menentukan prioritas penanganan kerentanan, melakukan penanganan terhadap kerentanan dalam bentuk remediasi dan mitigasi kerentanan, melakukan verifikasi terhadap langkah penanganan yang diambil dan memberikan laporan hasil penanganan kerentanan, serta melakukan evaluasi terhadap penanganan kerentanan yang dilakukan untuk mendapatkan pembelajaran yang dapat dipelajari dari adanya kerentanan tersebut.

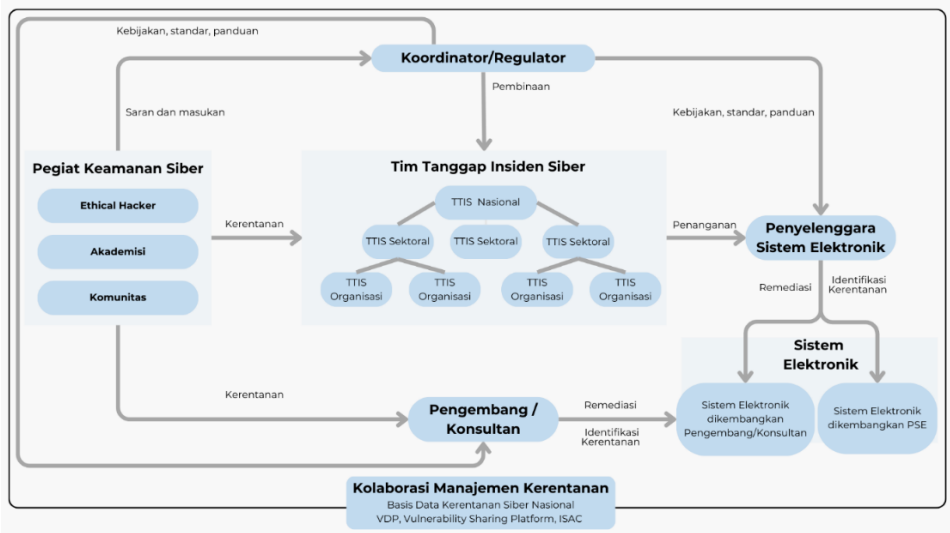
Bagian ketiga dari kerangka kerja menjelaskan sumber informasi kerentanan yang dapat diperoleh untuk melakukan identifikasi terhadap kerentanan pada aset. Sumber-sumber tersebut di antaranya adalah *vulnerability assessment* dan *penetration testing*, *vulnerability disclosure program/bug bounty*, *Vendor Advisory*, *threat intelligence*, dan *call center*. Banyaknya sumber informasi kerentanan yang dapat digunakan ini diharapkan dapat menciptakan kolaborasi di level nasional seperti

Vulnerability Sharing Platform dengan berbagai layanan manajemen kerentanan.

Bagian keempat dari kerangka kerja mendefinisikan setiap pihak yang terlibat dalam proses manajemen kerentanan. Bagian ini bertujuan untuk mengidentifikasi pihak-pihak yang terkait dalam manajemen kerentanan serta tugas dan tanggung jawab setiap pihak dalam siklus manajemen kerentanan tersebut. Pihak yang dimaksud dapat berupa individu tertentu atau organisasi, penyelenggara sistem elektronik, pengguna, pengembang/Konsultan, Komunitas Keamanan Siber, Koordinator dan Regulator, serta TTIS.

B. Kolaborasi Manajemen Kerentanan pada Tingkat Nasional

Manajemen kerentanan membutuhkan upaya terkoordinasi di seluruh proses rantai pasokan untuk secara efektif mengurangi risiko terkait kerentanan pada perangkat lunak dan sistem. Setiap pemangku kepentingan dalam ekosistem ini memiliki tanggung jawab yang berbeda-beda, dan kolaborasi di antara mereka sangat penting, mulai dari tahap identifikasi dan remediasi kerentanan hingga langkah-langkah selanjutnya. Kolaborasi ini dapat diwujudkan dalam berbagai program bersama seperti *Vulnerability Disclosure Program*, *Vulnerability Sharing Platform*, maupun *Information Sharing and Analysis Center* (ISAC).



Gambar 8. Kolaborasi Manajemen Kerentanan

Gambar 8 menunjukkan skema alur kolaborasi Manajemen Kerentanan di tingkat nasional. Koordinator/Regulator memiliki fungsi pembinaan serta penyusunan kebijakan, standar, atau panduan yang dapat dijadikan acuan oleh berbagai pihak, seperti Penyelenggara Sistem Elektronik (PSE) dan Pengembang/Konsultan. Di samping itu, peran utama Koordinator/Regulator adalah mengkoordinasikan setiap pihak yang terlibat agar dapat menjalankan peran dan tugas nya masing-masing dengan baik.

Pegiat Keamanan Siber juga memainkan peran penting dalam Manajemen Kerentanan. Pegiat Keamanan Siber yang terdiri dari *ethical hacker,* akademisi, atau komunitas dapat memberikan saran dan masukan terhadap Koordinator/Regulator mengenai kebijakan, kolaborasi, kegiatan yang dapat mendukung proses manajemen kerentanan. Selain itu, kerentanan yang ditemukan oleh Pegiat keamanan siber, dapat dilaporkan kepada Tim Tanggap Insiden Siber (TTIS) atapun Pengembang. Konsultan melalui jalur yang sudah tersedia. Seperti jalur *Vulnerability Disclosure Program* atau *Bug Bounty Program.*

Selanjutnya, pada sebuah organisasi, TTIS menjalankan fungsi manajemen kerentan di sisi internal organisasi. TTIS juga menjadi pintu masuk bagi organisasi untuk menerima laporan kerentanan dari pihak eksternal. Sehingga TTIS dapat melakukan identifikasi kerentanan baik yang bersumber dari eksternal, maupun dari internal TTIS yang dilakukan dengan cara pengujian keamanan pada Sistem Elektronik milik organisasi / PSE.

Di sisi lain, Pengembang/Konsultan juga memilki kewajiban untuk menjalankan manajemen kerentanan khususnya pada Produk yang digunakan oleh PSE. Produk ini dapat berupak perangkat keras ataupun perangkat lunak. Pengembang/Konsultan dapat menerima laporan kerentanan dari pihak eksternal, selain itu Pengembang/Konsultan juga memiliki kewajiban untuk melakukan identifikasi kerentanan secara internal lewat *Vulnerability Assessment* atau *Penetration Testing* secara berkala. Selanjutnya, pengembang/konsultan memiliki kewajiban untuk memberikan imbauan kerentanan kepada seluruh pengguna, apabila ditemukan kerentanan pada produk yang dikelola.

Seluruh *input* terkait kerentanan bermuara pada Sistem Elektronik yang dikelola oleh Penyelenggara Sistem Elektronik. Dengan adanya kolaborasi antar pihak, diharapkan kerentanan dapa diidentifikasi dengan maksimal, kemudian PSE dapat menangani kerentanan tersebut dengan baik. Dalam melakukan penanganan kerentanan, PSE juga dapat berkolaborasi dengan Pengembang/Konsultan serta TTIS untuk mengambil langkah yang tepat dan terukur dalam menangani kerentanan yang ada. Proses Manajemen Kerentanan pada organisasi secara lebih mendalam dibahas pada BAB V dan BAB VI buku ini.

Dengan adanya konsep kolaborasi ini, diharapkan dapat meningkatkan pelaksanaan manajemen kerentanan secara nasional. Tujuan utamanya adalah menciptakan Manajemen Kerentanan tingkat nasional yang terpadu dan efisien, selain itu diharapkan ke depannya dapat tersedia basis data kerentanan siber nasional. Basis data ini diharapkan dapat menjadi acuan bagi setiap pemangku kepentingan dalam melakukan penanganan serta pencegahan kerentanan.

Kolaborasi juga dapat diwujudkan dalam bentuk program atau platform, seperti program pengungkapan kerentanan secara sukarela (*Vulnerability Disclosure Program*) atau *Bug Bounty Program*, juga tersedianya platform berbagi informasi kerentanan (*Vulnerability Sharing Platfrom*).

C. Peran Setiap Pemangku Kepentingan pada Manajemen Kerentanan Tingkat Nasional

Koordinator dan Regulator

Koordinator dan regulator dalam konteks Indonesia adalah Pemerintah atau dalam hal ini BSSN. Koordinator dan regulator berperan untuk menyediakan kerangka kerja manajemen kerentanan secara nasional dan melakukan pembinaan kepada TTIS baik TTIS nasional, sektoral, atau organisasi terkait pelaksanaan manajemen kerentanan. Koordinator dan regulator juga dapat memberlakukan persyaratan untuk praktik manajemen kerentanan di TTIS sektor privat agar dapat terhubung dengan pelaksanaan manajemen kerentanan secara nasional. Koordinator dan regulator melakukan pembinaan ke TTIS. Sedangkan untuk PSE dan pengembang/konsultan, koordinator dan regulator mengeluarkan kebijakan, standar dan panduan yang diacu oleh organisasi dalam penerapan manajemen kerentanan.

Tim Tanggap Insiden Siber (TTIS)

TTIS terdiri atas TTIS nasional, sektoral, dan organisasi. TTIS melakukan penanganan insiden siber melalui beberapa hal sebagai berikut (BSSN, 2021):

1) Penanggulangan dan pemulihan insiden siber;
2) Penyampaian informasi insiden siber kepada pihak terkait; dan

3) Diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari insiden siber.

Dalam melakukan penanganan insiden siber, TTIS memiliki fungsi paling sedikit:

1) Pemberian peringatan terkait keamanan siber;
2) Perumusan panduan teknis penanganan insiden siber;
3) Pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
4) Pemilahan insiden siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan insiden siber yang akan ditangani;
5) Penyelenggaraan koordinasi penanganan insiden siber kepada pihak yang berkepentingan; dan
6) Penyelenggaraan fungsi lainnya sesuai kebutuhan.

Fungsi lainnya meliputi hal-hal berikut:

1) Penanganan kerentanan sistem elektronik;
2) Penanganan artefak digital;
3) Pemberitahuan hasil pengamatan potensi ancaman;
4) Pendeteksian serangan;
5) Analisis risiko keamanan siber;
6) Konsultasi terkait kesiapan penanganan insiden siber; dan/atau
7) Pembangunan kesadaran dan kepedulian terhadap keamanan siber.

TTIS sektoral, TTIS organisasi yang dibentuk oleh Penyelenggara IIV, dan TTIS organisasi yang dibentuk oleh Penyelenggara Sistem Elektronik selain Penyelenggara IIV wajib melakukan registrasi kepada TTIS nasional. Registrasi ini bertujuan untuk mendapatkan informasi yang valid mengenai profil TTIS sektoral dan organisasi, mempermudah koordinasi pada saat penanganan insiden siber antar-TTIS, dan mempermudah penyampaian informasi terkait ancaman, kerentanan, serta serangan siber kepada pihak yang berkepentingan.

1) TTIS Nasional

a. Keanggotaan

Keanggotaan TTIS nasional yang terdiri atas perwakilan:

- Badan;
- Kementerian atau Lembaga;
- Penyelenggara IIV; dan
- Penyelenggara Sistem Elektronik selain Penyelenggara IIV.

b. Kegiatan yang dilakukan

Dalam melaksanakan tugas dan menyelenggarakan fungsinya, TTIS nasional melakukan kegiatan sebagai berikut:

- Registrasi dan penerbitan surat tanda register TTIS sektoral dan organisasi;
- Pembangunan dan pengelolaan pangkalan data insiden siber dari seluruh TTIS yang teregister dan informasi mengenai insiden siber di tingkat nasional;
- Penghubung dengan negara lain dalam penanganan insiden siber;
- Penyusunan pilar strategi dan program kegiatan TTIS nasional;
- Forum analisis dan berbagi informasi keamanan siber dengan TTIS yang teregistrasi;
- Pembangunan program berbagi pengetahuan atau pengalaman terkait dengan penanganan insiden siber kepada seluruh TTIS yang teregistrasi.

2) TTIS Sektoral

a. Keanggotaan

Keanggotaan TTIS sektoral yang terdiri atas perwakilan:

- Kementerian atau Lembaga;
- Penyelenggara IIV; dan
- Penyelenggara Sistem Elektronik selain Penyelenggara IIV.

b. Kegiatan yang dilakukan

Dalam melaksanakan tugas dan menyelenggarakan fungsinya, TTIS sektoral melakukan kegiatan sebagai berikut:

- Forum analisis dan berbagi informasi keamanan siber dengan TTIS di bawahnya; dan
- Uji komunikasi dengan TTIS organisasi yang ada di sektornya

3) TTIS Organisasi

TTIS organisasi dibentuk oleh setiap Penyelenggara IIV. TTIS organisasi dapat menyelenggarakan kegiatan forum analisis dan berbagi informasi keamanan siber lintas sektor.

TTIS bertanggung jawab untuk menerima, menganalisis, dan menindaklanjuti informasi terkait kerentanan yang disampaikan oleh berbagai pihak, termasuk dari komunitas pegiat keamanan siber. Tugas utama TTIS mencakup pengumpulan data, verifikasi kerentanan, serta koordinasi penanganan dengan penyelenggara sistem elektronik yang bertanggung jawab atas sistem elektronik yang teridentifikasi memiliki kerentanan. TTIS juga berperan dalam memastikan komunikasi yang efektif antara semua pihak yang terlibat, sehingga penanganan kerentanan dapat dilakukan dengan cepat dan tepat. Dalam kolaborasi manajemen kerentanan, TTIS memiliki beeberapa tugas dan peran sebagai berikut:

1) Penerimaan Kerentanan: TTIS menerima laporan kerentanan dari koordinator/regulator dan komunitas pegiat keamanan siber.
2) Verifikasi dan Analisis: Setelah menerima laporan, TTIS melakukan verifikasi dan analisis untuk memastikan validitas kerentanan yang dilaporkan.
3) Koordinasi dengan PSE: TTIS menghubungi PSE yang terkait untuk menyampaikan hasil analisis kerentanan dan mengkoordinasikan langkah penanganan yang diperlukan.
4) Pembinaan oleh Koordinator: TTIS menerima pembinaan berkelanjutan dari koordinator atau regulator untuk

meningkatkan kemampuan dan efektivitas dalam manajemen kerentanan.

5) Pelaporan dan Tindak Lanjut: Setelah kerentanan ditangani, TTIS menyusun laporan mengenai proses penanganan dan hasilnya, yang kemudian disampaikan kepada koordinator/regulator.
6) Pemantauan Berkelanjutan: TTIS terus memantau potensi kerentanan baru dan melakukan evaluasi terhadap efektivitas langkah-langkah mitigasi yang telah dilakukan.
7) Kolaborasi dengan Komunitas: TTIS membuka jalur komunikasi dengan komunitas pegiat keamanan siber untuk menerima masukan serta berbagi informasi terkait kerentanan yang mungkin belum teridentifikasi.

Pegiat Keamanan Siber

Pegiat Keamanan Siber adalah kelompok/individu dalam proses identifikasi kerentanan. Pegiat keamanan siber terdiri dari beberapa pihak yaitu peretas etis, akademisi, dan komunitas. Pegiat keamanan siber dapat digolongkan menjadi 2 bagian yaitu pegiat keamanan siber internal yang merupakan karyawan dari organisasi itu sendiri dan pegiat keamanan siber eksternal yang meliputi peretas etis (*ethical hacker*), akademisi berupa sivitas akademika atau peneliti keamanan siber, dan komunitas keamanan siber yang berperan secara aktif untuk mendukung manajemen kerentanan. Peranan pegiat keamanan siber adalah mengidentifikasi kerentanan melalui berbagai cara seperti uji penetrasi sistem keamanan, analisis kode, atau metode investigasi lainnya. Pegiat keamanan siber bertanggung jawab untuk melaporkan kerentanan yang ditemukan kepada TTIS dengan cara sebagai berikut:

1) Mengirimkan informasi kerentanan secara detail ke e-mail pelaporan resmi;
2) Berpartisipasi aktif dalam mengikuti *bug bounty* yang diselenggarakan;

3) Melaporkan kerentanan kepada Koordinator/Regulator seperti BSSN.

Kualitas, akurasi, dan ketepatan waktu laporan pegiat keamanan siber sangat penting karena faktor-faktor ini mempengaruhi langkah-langkah selanjutnya dalam proses manajemen kerentanan.

Pegiat keamanan siber wajib memiliki etika dengan tidak melakukan segala perbuatan yang disebutkan di dalam Pasal 27 hingga pasal 37 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik baik secara sengaja ataupun tidak. Langkah-langkah yang bisa dilakukan pegiat keamanan siber untuk mewujudkan rantai ekosistem manajemen kerentanan yang sehat adalah dengan mengungkapkan kerentanan secara bertanggung jawab (*responsible disclosure*) yang meliputi tahapan yang disajikan pada Gambar 9.

Gambar 9. *Responsible Disclosure*

Gambar 9 dapat dirinci sebagai berikut:

1. Pegiat keamanan siber menemukan potensi kerentanan pada suatu sistem atau berpartisipasi aktif dalam program *bug bounty* yang diselenggarakan oleh sebuah pengelola sistem.
2. Pegiat keamanan siber melaporkan temuan kepada pihak yang berwenang (misalnya tim keamanan organisasi atau penyedia layanan) tanpa mengungkapkan informasi tersebut kepada publik atau pihak ketiga.
3. Pegiat keamanan siber dan pengelola sistem bekerja sama untuk memahami dan memperbaiki kerentanan.
4. Pegiat keamanan siber memberikan jangka waktu tertentu kepada pengelola sistem untuk memperbaiki kerentanan sebelum mereka mempublikasikan laporan lengkap terkait kerentanan tersebut dan dilarang keras untuk mengeksploitasi kerentanan yang ditemukan dengan semena-mena.

5. Setelah kerentanan diperbaiki dan sudah ditangani, pegiat keamanan siber dapat mempublikasikan laporan teknis tentang kerentanan untuk membantu komunitas keamanan siber agar dapat belajar dari temuan tersebut.

Pengembang/Konsultan

Pengembang/Konsultan merupakan pihak produsen perangkat keras, pengembang perangkat lunak, dan penyedia layanan yang digunakan oleh Penyelenggara Sistem Elektronik (PSE). Pihak pengembang atau konsultan memainkan peran penting dalam manajemen kerentanan. Pasalnya, kerentanan dapat ditemukan pada produk perangkat TI milik pengembang/konsultan atau sistem yang dikelolanya, yang dapat menimbulkan risiko pada Sistem Elektronik yang menggunakan sistem/perangkat yang rentan tersebut.

Penyelenggara Sistem Elektronik (PSE) memerlukan peran aktif dari pengembang/konsultan terkait untuk melakukan manajemen kerentanan pada produk atau sistem yang dikelolanya. Sehingga dalam siklus manajemen kerentanan di tingkat nasional, pengembang/konsultan juga memiliki peranan yang krusial, yakni memastikan para pengguna produk TI atau layanannya, dalam hal ini PSE, mendapatkan informasi yang cukup dan segera ketika ditemukan adanya kerentanan. Sehingga dapat memperkecil risiko kerentanan tersebut dieksploitasi pihak yang tidak bertanggungjawab.

Peran kolaborasi pengembang/ konsultan ini mencakup beberapa aspek, yaitu aspek kesadaran akan kerentanan (*vulnerability awareness*), proses verifikasi, perbaikan, pengungkapan, dan mitigasi risiko kerentanan selama siklus hidup dari sebuah produk perangkat TI.

Penyelenggara Sistem Elektronik

Penyelenggara Sistem Elektronik (PSE) merupakan setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik

sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain (Presiden Indonesia, 2019). PSE terdiri dari PSE lingkup publik dan lingkup privat. PSE lingkup publik terdiri atas instansi pemerintah dan institusi yang ditunjuk oleh instansi pemerintah. Setiap PSE harus menyelenggarakan sistem elektronik secara andal dan aman serta memiliki tanggung jawab terhadap operasional sistem elektronik miliknya.

Dalam perannya terhadap kolaborasi manajemen kerentanan, PSE merupakan pihak yang bertanggung jawab atas penyelenggaraan sistem elektronik. Sistem elektronik tersebut dapat dikembangkan oleh pihak pengembang/konsultan dan dikembangkan secara mandiri. Selain penyelenggaraan sistem elektronik, peran PSE dalam kolaborasi manajemen kerentanan adalah dengan melakukan identifikasi kerentanan berupa proses VA/PT terhadap sistem elektronik yang dikelola. VA/PT dilakukan oleh tim internal PSE sebagai upaya identifikasi dini kerentanan yang dapat berisiko pada keberlangsungan penyelenggaraan sistem elektronik. Pada proses VA/PT internal, kerentanan yang ditemukan dapat segera dilakukan perbaikan oleh PSE secara mandiri. Ketika kerentanan ditemukan dalam sistem elektronik PSE melaluai pegiat keamanan siber, PSE mendapatkan layanan dari TTIS berupa penanganan kerentanan sehingga PSE dapat menerapkan remediasi kerentanan pada sistem elektronik miliknya. PSE yang memiliki sistem elektronik dari pengembang/konsultan juga dapat melakukan koordinasi agar pengembang/konsultan dapat menerapkan remediasi terhadap sistem elektronik milik PSE yang telah dikembangkan.

Dalam menerapkan remediasi, PSE perlu mengevaluasi risiko kerentanan dalam konteks operasional yang spesifik, memprioritaskan kerentanan berdasarkan faktor seperti tingkat kritis, serta menerapkan patch atau langkah mitigasi yang diperlukan. Selain itu, pemantauan berkelanjutan terhadap sistem menjadi krusial untuk mendeteksi potensi eksploitasi, guna menjaga agar kerentanan tidak mengganggu

operasi. Pengelolaan aset yang efektif, penilaian risiko yang komprehensif, serta kemampuan tanggap insiden yang cepat sangat penting untuk menghadapi ancaman baru secara efisien.

BAB IV
BENCHMARK ORGANISASI DAN TATA KELOLA TERKAIT MANAJEMEN KERENTANAN

The cybersecurity landscape is continuously evolving. Staying ahead of the threats means staying on top of the latest developments

- Raj Samani

A. *Benchmark* Organisasi dalam Praktik Manjemen Kerentanan

Dalam manajemen kerentanan, peran TTIS sangat penting untuk mengidentifikasi, menganalisis, dan merespons kerentanan keamanan siber di dalam sebuah organisasi. TTIS bertanggung jawab untuk mengoordinasikan respons terhadap insiden keamanan yang mungkin timbul akibat kerentanan yang belum ditangani, serta memastikan bahwa langkah-langkah mitigasi yang tepat diterapkan secara efektif. Agar manajemen kerentanan dapat berfungsi secara optimal, diperlukan dukungan yang kuat dari organisasi, termasuk dalam hal tata kelola, kebijakan, sumber daya, dan teknologi. Organisasi harus menyediakan sumber daya yang memadai untuk pengelolaan kerentanan, seperti tenaga ahli, alat deteksi dan mitigasi kerentanan, serta prosedur yang jelas untuk penilaian dan pengelolaan risiko. Selain itu, dukungan dari pimpinan dan kolaborasi antar-departemen juga penting untuk memastikan bahwa manajemen kerentanan dilakukan secara menyeluruh dan berkesinambungan, guna melindungi infrastruktur dan data kritis organisasi dari ancaman siber yang terus berkembang.

Pada bagian ini dibahas beberapa praktik manajemen kerentanan pada negara-negara terdepan dalam keamanan siber. Negara-negara tersebut adalah Amerika Serikat, Jepang, Uni Eropa, Jerman dan Australia. Pemilihan kelima negara tersebut didasarkan pada fakta bahwa masing-masing mencerminkan beragam pendekatan dan praktik dalam manajemen kerentanan, serta menawarkan pandangan yang komprehensif dan bervariasi tentang strategi keamanan siber di tingkat global.

Amerika Serikat

Di Amerika Serikat, /*United States Computer Emergency Readiness Team* (US-CERT) (US-CERT, 2020), yang merupakan bagian dari *Cybersecurity and Infrastructure Security Agency* (CISA) di bawah Departemen Keamanan Dalam Negeri (Department of Homeland Security-DHS), memiliki fokus utama pada perlindungan infrastruktur kritis nasional, termasuk sektor energi, keuangan, dan komunikasi. Tim ini menyediakan dukungan respons insiden dan berbagi informasi keamanan siber dengan organisasi publik dan swasta di seluruh Amerika Serikat. US-CERT berkolaborasi dengan sektor swasta, lembaga pemerintah, dan mitra internasional untuk memperkuat keamanan siber secara menyeluruh. Di tingkat global, US-CERT sering dijadikan acuan dalam praktik terbaik untuk perlindungan infrastruktur kritis nasional. Sebagai bagian dari CISA, US-CERT memainkan peran kunci dalam manajemen kerentanan di Amerika Serikat dengan memantau dan menganalisis kerentanan yang dapat mempengaruhi infrastruktur kritis nasional (CISA, 2020). US-CERT menggunakan berbagai sumber intelijen untuk mengidentifikasi kerentanan yang baru muncul dan melakukan penilaian risiko terhadap potensi dampaknya. Setelah kerentanan diidentifikasi, saran yang diberikan mencakup informasi tentang cara mitigasi, termasuk rekomendasi untuk *patching* dan perlindungan sistem. Kerja sama dengan sektor swasta dilakukan untuk memastikan bahwa kerentanan yang ditemukan segera ditangani, serta memberikan panduan kepada organisasi dalam menerapkan solusi mitigasi yang tepat. Pendekatan ini mencakup penyebaran informasi dan panduan teknis secara luas untuk membantu organisasi mengelola dan mengatasi kerentanan yang terdeteksi.

National Vulnerability Database (NVD) (Booth et al., 2013; NIST, 2024) juga memainkan peran krusial dalam manajemen kerentanan di Amerika Serikat. NVD adalah basis data yang dikelola oleh *National Institute of Standards and Technology* (NIST) dan berfungsi sebagai pusat penyimpanan informasi tentang kerentanan perangkat lunak dan perangkat keras. NVD menyediakan data yang dikategorikan berdasarkan *Common Vulnerabilities and Exposures* (CVE) yang terdaftar

dan mencakup detail teknis, dampak, dan solusi mitigasi untuk setiap kerentanan. Data yang disediakan oleh NVD sangat penting untuk penilaian risiko dan perencanaan mitigasi di berbagai organisasi, serta untuk pengembangan kebijakan keamanan siber di seluruh Amerika Serikat.

Jepang

Japan *Computer Emergency Response Team Coordination Center* (JPCERT/CC) adalah entitas swasta yang berfungsi sebagai CSIRT nasional Jepang. Meskipun bukan lembaga pemerintah, JPCERT/CC bekerja erat dengan pemerintah Jepang dalam hal keamanan siber (JPCERT/CC, 2024). Fokus utama JPCERT/CC adalah pengumpulan, analisis, dan distribusi informasi terkait insiden keamanan siber, serta memberikan dukungan teknis dan koordinasi antar-CSIRT di Jepang. Dalam hal manajemen kerentanan, JPCERT/CC secara aktif memantau dan menganalisis kerentanan yang dapat memengaruhi sistem TI di Jepang. Data tentang kerentanan dikumpulkan dari berbagai sumber, termasuk laporan keamanan dan hasil penelitian, untuk menyusun *advisories* dan panduan mitigasi yang membantu organisasi menangani risiko tersebut. JPCERT/CC juga bekerja sama dengan pengembang dan penyedia layanan untuk memastikan bahwa solusi mitigasi, seperti *patch*, tersedia dan diterapkan dengan efektif. Melalui jaringan kolaborasi yang kuat baik di tingkat nasional maupun internasional, serta keterlibatannya dalam forum CSIRT regional di Asia, JPCERT/CC menekankan pentingnya kemitraan antara sektor swasta dan pemerintah serta peningkatan kesadaran dan edukasi tentang keamanan siber.

Uni Eropa

CERT-EU (CERT-EU, 2024) adalah CSIRT yang didirikan untuk mendukung institusi, badan, dan agensi Uni Eropa. Beroperasi di bawah Komisi Eropa, CERT-EU bertugas melindungi infrastruktur TI dari

ancaman siber yang dapat memengaruhi operasi Uni Eropa. Selain itu, CERT-EU bekerja sama dengan CSIRT nasional dari negara anggota Uni Eropa dan *European Union Agency for Cybersecurity* (ENISA) untuk memperkuat keamanan siber di tingkat regional. Aktivitas termasuk latihan keamanan siber besar dan berbagi informasi dengan mitra internasional, menjadikannya aktor penting dalam keamanan siber Eropa.

Jerman

CERT-Bund, yang dikelola oleh *Federal Office for Information Security* (BSI), merupakan bagian dari Kementerian Dalam Negeri Jerman. CERT-Bund (CERT-Bund, 2024) bertanggung jawab untuk memantau, menganalisis, dan merespons ancaman siber yang dapat memengaruhi infrastruktur kritis dan sistem pemerintahan Jerman. Melalui CERT-Bund, BSI menjalin kerja sama yang erat dengan sektor swasta, CSIRT lainnya di Eropa, dan institusi keamanan siber internasional. Pendekatan yang diterapkan terstruktur dan formal, dengan penekanan pada kepatuhan regulasi serta penerapan strategi keamanan siber nasional yang ketat untuk memastikan respons yang cepat dan efektif terhadap ancaman siber.

Australia

Australian Computer Emergency Response Team (AusCERT) adalah lembaga keamanan siber yang berfokus pada penyediaan layanan tanggap insiden serta dukungan teknis terkait keamanan informasi. Mengacu pada dokumen RFC 2350 (AusCERT, 2024), AusCERT bertugas menjelaskan prosedur dan kebijakan yang diterapkan untuk menangani insiden siber. Layanan yang ditawarkan mencakup kegiatan identifikasi, penanganan, dan mitigasi insiden dengan tujuan melindungi infrastruktur informasi yang kritis. Selain itu, dokumen tersebut menyoroti peran AusCERT dalam memastikan koordinasi dan

komunikasi yang efektif antara pihak-pihak terdampak, baik di tingkat nasional maupun internasional.

Di samping tanggap insiden, AusCERT juga memainkan peran krusial dalam manajemen kerentanan, yang merupakan pilar utama keamanan siber. Proses manajemen kerentanan meliputi identifikasi, evaluasi, dan perbaikan kerentanan yang terdapat pada perangkat lunak, perangkat keras, dan jaringan sistem. Melalui layanan ini, AusCERT bekerja sama dengan berbagai organisasi untuk mengelola kerentanan serta mencegah eksploitasi yang berpotensi dilakukan oleh pihak berbahaya. Dengan pendekatan menyeluruh, termasuk pemantauan berkelanjutan dan penerapan *patch* keamanan, manajemen kerentanan yang dilakukan oleh AusCERT bertujuan untuk memperkuat ketahanan organisasi dalam menghadapi ancaman siber yang semakin kompleks. Perbandingan kelima negara di atas disajikan pada Tabel 1.

Tabel 1. Perbandingan lima negara

Negara	CSIRT	Fokus Utama	Manajemen Kerentanan
Amerika Serikat	US-CERT	Perlindungan infrastruktur kritis nasional (energi, keuangan, komunikasi); dukungan respons insiden; berbagi informasi keamanan siber	Pemantauan dan analisis kerentanan, kolaborasi dengan sektor swasta, mitigasi dan *patch*ing
Jepang	JPCERT/CC	Pengumpulan, analisis, distribusi informasi terkait insiden siber; dukungan teknis dan koordinasi CSIRT nasional	Pemantauan, analisis, dan advisories; kerja sama dengan pengembang dan penyedia layanan

Negara	CSIRT	Fokus Utama	Manajemen Kerentanan
Uni Eropa	CERT-EU	Perlindungan infrastruktur TI di institusi Uni Eropa; berbagi informasi, koordinasi dengan CSIRT nasional di negara anggota	Berbagi informasi, koordinasi, dan partisipasi dalam forum keamanan siber
Jerman	CERT-Bund	Memantau, menganalisis, dan merespons ancaman siber; kerja sama dengan sektor swasta dan CSIRT internasional	Kerja sama dengan sektor swasta dan internasional, respons cepat terhadap ancaman kerentanan
Australia	AusCERT	Tanggap insiden, mitigasi, dan perlindungan infrastruktur kritis; dukungan teknis dan koordinasi nasional dan internasional	Identifikasi, evaluasi, perbaikan kerentanan, pemantauan berkelanjutan, dan *patch*ing

B. *Standar* Internasional dan Panduan Praktik Tata Kelola Manajemen Kerentanan

Beberapa standar internasional dan panduan praktik terbaik yang diterbitkan oleh organisasi terkemuka menawarkan pedoman komprehensif untuk mengatur dan mengelola manajemen kerentanan. Berikut ini adalah panduan yang diterbitkan oleh beberapa organisasi internasional:

National Institute of Standards and Technology (NIST)[13]

NIST, sebagai lembaga non-regulasi dari Departemen Perdagangan Amerika Serikat, memainkan peran penting dalam menetapkan standar dan panduan untuk keamanan siber, termasuk manajemen kerentanan. NIST mengembangkan kerangka kerja sebagai berikut:

1) NIST *Special Publication* 800-40 *Revision* 4: *Guide to Enterprise Patch Management Planning* - Panduan ini membahas manajemen tambalan dan cara yang efektif untuk mengelola kerentanan melalui pembaruan perangkat lunak.
2) NIST *Special Publication* 800-53 *Revision* 5: *Security and Privacy Controls for Information Systems and Organizations* - Dokumen ini mencakup kontrol keamanan dan privasi, termasuk yang berkaitan dengan manajemen kerentanan. Kontrol tersebut bisa mencakup pembaruan sistem, pengujian keamanan, dan pemantauan kerentanan.
3) NIST *Special Publication* 800-115: *Technical Guide to Information Security Testing and Assessment* - Panduan ini memberikan wawasan tentang pengujian keamanan dan penilaian yang dapat membantu dalam mengidentifikasi dan mengelola kerentanan.
4) NIST *Special Publication* 800-30 *Revision* 1: *Guide for Conducting Risk Assessments* - Meskipun fokus utamanya adalah penilaian risiko, panduan ini juga memberikan kerangka kerja untuk mengidentifikasi dan mengelola kerentanan sebagai bagian dari proses manajemen risiko.
5) NIST *Special Publication* 800-61 Revision 2: "*Computer Security Incident Handling Guide*" – Ini memberikan panduan untuk menangani insiden keamanan, termasuk aspek terkait dengan kerentanan.

Kerangka kerja yang diberikan oleh NIST dirancang untuk integrasi yang mudah dengan kebijakan dan prosedur keamanan yang ada di

[13] https://www.nist.gov/

organisasi, memungkinkan pendekatan yang fleksibel namun sistematis dalam manajemen kerentanan. Melalui publikasinya, NIST membantu organisasi dalam memahami risiko keamanan, menerapkan kontrol yang tepat, dan memelihara postur keamanan yang tangguh melalui penerapan terbaik dan penilaian yang terus-menerus.

European Union Agency for Cybersecurity (ENISA)[14]

ENISA berperan sebagai pusat keahlian di Eropa, fokus pada peningkatan keamanan siber di seluruh Uni Eropa. Melalui panduan dan alatnya, ENISA mendukung negara-negara anggota, institusi swasta, serta bisnis dalam meningkatkan kemampuan mereka untuk mencegah, mendeteksi, dan merespons insiden siber, termasuk manajemen kerentanan. Organisasi ini mengusulkan kerangka kebijakan yang memfasilitasi pertukaran informasi dan praktik terbaik antara negara anggota.

Dengan berfokus pada kolaborasi lintas batas dan peningkatan kapabilitas keamanan siber, ENISA juga mendukung inisiatif penelitian dan pengembangan yang bertujuan mengidentifikasi dan mengatasi celah keamanan baru. Misalnya, ENISA menyelenggarakan latihan keamanan siber tahunan dan lokakarya yang membantu memperkuat kerja sama internasional dan kesiapan terhadap serangan siber, sekaligus meningkatkan efektivitas manajemen kerentanan dalam berbagai konteks.

Forum of Incident Response and Security Teams (FIRST)[15]

FIRST adalah forum global yang terdiri dari tim respons keamanan dan insiden dari lebih dari 80 negara. Organisasi ini berfokus pada peningkatan kerjasama dan koordinasi dalam menanggapi insiden keamanan siber, serta manajemen kerentanan. FIRST menyediakan

[14] https://www.enisa.europa.eu/

[15] https://www.first.org/about/mission

standar, alat, dan praktik terbaik untuk meningkatkan kemampuan anggotanya dalam menangani insiden siber secara efektif.

Anggota FIRST, yang meliputi pemerintah, universitas, dan korporasi, saling berbagi pengetahuan dan sumber daya tentang insiden keamanan terbaru, kerentanan, dan ancaman siber. Melalui pertemuan, konferensi, dan sistem pelaporan kerentanan bersama, FIRST memungkinkan pertukaran informasi yang cepat dan efisien, memperkuat kemampuan global untuk merespons dan mengelola risiko keamanan siber secara lebih proaktif.

Center for Internet Security (CIS)[16]

CIS adalah organisasi non-profit yang berdedikasi menyediakan solusi keamanan siber bagi sektor publik dan swasta. Entitas ini dikenal luas melalui CIS *Benchmarks*[17] dan CIS Controls[18], yaitu serangkaian standar dan rekomendasi yang dirancang untuk meningkatkan postur keamanan organisasi. CIS *Controls* secara khusus menangani manajemen kerentanan dengan menyediakan panduan langkah demi langkah yang membantu organisasi dalam mengidentifikasi, menilai, dan mengurangi kerentanan yang ada. Dengan mengikuti standar ini, organisasi dapat mengadopsi praktik terbaik untuk memperkuat keamanan sistem mereka serta meminimalkan risiko terhadap potensi ancaman siber. Selain menyediakan *Benchmark*, CIS juga menawarkan alat dan layanan yang membantu organisasi dalam menerapkan kontrol keamanan yang efektif dan efisien. Dengan fokus pada praktik terbaik industri dan kerja sama komunitas, CIS memfasilitasi pembelajaran dan

[16] https://www.cisecurity.org/

[17] https://www.cisecurity.org/cis-benchmarks

[18] https://www.cisecurity.org/controls

pertukaran pengetahuan antar anggota, yang meliputi berbagai industri dan pemerintahan, untuk secara kolektif meningkatkan keamanan siber.

International Organization for Standardization (ISO)[19]

ISO, sebagai organisasi internasional yang mengembangkan dan menerbitkan standar global, menawarkan sejumlah standar yang penting untuk sistem manajemen keamanan informasi. Dalam konteks manajemen kerentanan, berbagai standar ISO memberikan panduan yang signifikan untuk praktik keamanan informasi yang efektif. ISO/IEC 27001:2013 merupakan standar utama yang menetapkan persyaratan untuk sistem manajemen keamanan informasi (ISMS) dan mencakup berbagai aspek pengelolaan risiko, termasuk penanganan kerentanan. ISO/IEC 27002:2022 melengkapi ISMS dengan panduan praktis mengenai kontrol keamanan informasi, menekankan penerapan kontrol yang dapat mengatasi kerentanan dengan lebih efisien.

Selain itu, ISO/IEC 27005:2018 memperluas cakupan manajemen risiko keamanan informasi dengan fokus pada identifikasi dan mitigasi kerentanan sebagai bagian integral dari proses manajemen risiko. ISO/IEC 29147:2018 memberikan pedoman tentang cara menangani laporan kerentanan, mencakup prosedur untuk penanganan yang efektif. ISO/IEC 30111:2019 melengkapi panduan ini dengan prosedur untuk perbaikan dan resolusi kerentanan yang ditemukan. Secara keseluruhan, standar-standar ini membentuk kerangka kerja yang komprehensif, memfasilitasi identifikasi, penilaian, dan pengelolaan kerentanan, serta meningkatkan keamanan informasi dan perlindungan sistem secara keseluruhan.

MITRE[20]

[19] https://www.iso.org/home.html

[20] https://www.mitre.org/who-we-are/our-story

MITRE adalah organisasi yang mengelola dan mendukung berbagai inisiatif keamanan siber, termasuk *Common Vulnerabilities and Exposures* (CVE) dan *Common Weakness Enumeration* (CWE). CVE menyediakan identifikasi standar untuk kerentanan keamanan siber yang diketahui, memungkinkan pertukaran data antara berbagai produk keamanan dan memudahkan organisasi untuk menilai tingkat ancaman dari kerentanan yang ditemukan. CWE, di sisi lain, adalah daftar kondisi umum dalam kode yang dapat menyebabkan kerentanan.

Dengan menyediakan sumber daya ini, MITRE memainkan peran penting dalam memfasilitasi pengenalan dan penanganan kerentanan di seluruh industri. Organisasi ini juga terlibat dalam pengembangan kerangka kerja ATT&CK, yang digunakan untuk meningkatkan pemahaman tentang taktik, teknik, dan prosedur yang digunakan oleh para pelaku ancaman, sehingga membantu dalam mempersiapkan dan merespons ancaman siber secara lebih efektif.

Open Web Application Security Project (OWASP)[21]

OWASP menyediakan berbagai panduan yang sangat berguna untuk manajemen kerentanan dalam aplikasi web. Salah satu panduan utama adalah OWASP Top Ten, yang mengidentifikasi dan mendokumentasikan sepuluh risiko keamanan aplikasi web yang paling kritis. Panduan ini memberikan wawasan mendalam tentang kerentanan umum yang sering dimanfaatkan oleh penyerang, seperti injeksi, pelanggaran autentikasi, dan eksposur data sensitif. Dengan memahami dan menerapkan rekomendasi dari OWASP *Top Ten*, organisasi dapat mengurangi risiko yang terkait dengan kerentanan aplikasi web mereka secara signifikan. Panduan ini juga mencakup langkah-langkah mitigasi dan kontrol yang dapat diterapkan untuk memperbaiki kelemahan yang teridentifikasi.

[21] https://owasp.org/

Selain OWASP *Top Ten*, OWASP *Application Security Verification Standard* (ASVS) menyediakan kerangka kerja yang komprehensif untuk mengukur dan memverifikasi keamanan aplikasi. ASVS menawarkan serangkaian kontrol dan kriteria verifikasi yang dirancang untuk memastikan bahwa aplikasi memenuhi standar keamanan yang tinggi. Panduan ini mencakup berbagai tingkat verifikasi, dari pengujian dasar hingga evaluasi mendalam, untuk menilai kekuatan perlindungan terhadap kerentanan.

SANS *Institute*[22]

SANS *Institute* adalah lembaga riset dan pendidikan terkemuka di bidang keamanan informasi dan jaringan, yang menawarkan pelatihan dan sertifikasi ekstensif dalam berbagai topik keamanan siber, termasuk manajemen kerentanan. Institusi ini menggabungkan teori terbaru dengan praktik terbaik industri dan studi kasus untuk menyediakan pengetahuan praktis yang langsung dapat diterapkan oleh profesional di lapangan. Selain pelatihan, SANS juga menyediakan berbagai alat keamanan seperti poster dan lembar tips yang membantu profesional dalam tugas sehari-hari mereka. Melalui konferensi dan lokakarya yang rutin diadakan, SANS memfasilitasi pertukaran pengetahuan dan menawarkan sumber daya pendidikan terbaru untuk komunitas keamanan global.

Dalam konteks manajemen kerentanan, SANS Institute telah mengeluarkan panduan penting seperti SANS *Critical Security Controls* dan SANS Top 20 *Critical Security Controls*. Kontrol 4: *Vulnerability Assessment* dari SANS *Critical Security Controls* menekankan pemindaian kerentanan secara rutin, pembaruan, dan pemprioritasan kerentanan berdasarkan risiko, serta penerapan *patch* untuk mengurangi eksposur terhadap ancaman. Sementara itu, Kontrol 7: *Continuous Vulnerability Assessment and Remediation* dalam SANS Top

[22] https://www.sans.org/

20 *Critical Security Controls* menggarisbawahi pentingnya penilaian kerentanan yang berkelanjutan dan perbaikan yang cepat untuk menjaga ketahanan sistem. Panduan-panduan ini memberikan kerangka kerja yang praktis dan terstruktur untuk meningkatkan keamanan dengan fokus pada pemantauan, mitigasi, dan penanganan kerentanan, membantu organisasi membangun program manajemen kerentanan yang proaktif untuk meningkatkan keamanan informasi dan mitigasi risiko secara keseluruhan.

Australian Cyber Security Centre (ACSC)[23]

ACSC bertindak sebagai otoritas keamanan siber di Australia, menyediakan kepemimpinan, koordinasi, dan dukungan untuk mencegah dan merespons insiden keamanan siber di negara tersebut. Sebagai bagian dari kegiatan mereka, ACSC menyediakan panduan yang komprehensif untuk manajemen kerentanan, mendukung organisasi dan warga Australia dalam melindungi infrastruktur kritis dan informasi pribadi.

ACSC secara teratur memperbarui dan mengkomunikasikan ancaman siber melalui peringatan keamanan, panduan teknis, dan rekomendasi untuk praktik terbaik dalam manajemen kerentanan dan keamanan siber secara umum. Dengan menggabungkan sumber daya dari pemerintah, sektor privat, dan masyarakat, ACSC berupaya memperkuat ketahanan nasional terhadap ancaman siber, memastikan pendekatan yang lebih terkoordinasi dan efektif dalam manajemen kerentanan.

Tabel 2 merinci peranan, kerangka kerja, dan fokus pada manajemen kerentanan dari berbagai lembaga keamanan siber yang penting di tingkat global.

Tabel 2. Perbandingan Lembaga Keamanan Siber dan Pendekatan Manajemen Kerentanan

[23] https://www.cyber.gov.au/

No.	Lembaga	Peran Utama	Kerangka Kerja dan Panduan	Fokus pada Manajemen Kerentanan
1	NIST	Menetapkan standar dan panduan keamanan siber	▪ NIST SP 800-40: Patch management ▪ NIST SP 800-53: Security & Privacy Controls ▪ NIST SP 800-115: Security Testing ▪ NIST SP 800-30: Risk Assessment ▪ NIST SP 800-61: Incident Handling	Memfasilitasi identifikasi, pemantauan, dan mitigasi kerentanan melalui pendekatan sistematis dalam keamanan dan penilaian risiko.
2	ENISA	Peningkatan keamanan siber di Eropa	▪ Latihan keamanan tahunan ▪ Lokakarya peningkatan kapabilitas keamanan siber	Fokus pada kolaborasi lintas negara, berbagi praktik terbaik, dan mendukung penelitian untuk mengatasi celah keamanan baru.
3	FIRST	Forum respons keamanan global	▪ Standar dan alat respons insiden ▪ Konferensi dan pertukaran informasi	Memperkuat koordinasi global dalam menanggapi insiden keamanan dan mengelola kerentanan secara proaktif.
4	CIS	Solusi keamanan siber untuk sektor publik & swasta	▪ CIS Controls ▪ CIS Benchmarks	Panduan langkah demi langkah untuk mengidentifikasi, menilai, dan mengurangi kerentanan melalui penerapan standar terbaik.
5	ISO	Pengembangan standar global	▪ ISO/IEC 27001: ISMS ▪ ISO/IEC 27002: Practical Controls	Standar komprehensif untuk identifikasi, penilaian, dan mitigasi kerentanan dalam sistem

No.	Lembaga	Peran Utama	Kerangka Kerja dan Panduan	Fokus pada Manajemen Kerentanan
			▪ ISO/IEC 27005: Risk Management ▪ ISO/IEC 29147: Vulnerability Handling ▪ ISO/IEC 30111: Vulnerability Resolution	manajemen keamanan informasi.
6	MITRE	Pengelolaan CVE dan CWE	▪ CVE: Common Vulnerabilities and Exposures ▪ CWE: Common Weakness Enumeration ▪ ATT&CK Framework	Meningkatkan identifikasi dan penanganan kerentanan melalui daftar standar untuk kode yang rentan serta pemahaman tentang taktik serangan.
7	OWASP	Keamanan aplikasi web	▪ OWASP Top Ten ▪ ASVS (Application Security Verification Standard)	Panduan penting untuk mengurangi risiko kerentanan aplikasi web dengan kontrol dan langkah mitigasi terstruktur.
8	SANS Institute	Riset dan pendidikan keamanan siber	▪ SANS Critical Security Controls ▪ SANS Top 20 Critical Security Controls	Panduan untuk penilaian dan mitigasi kerentanan yang berkelanjutan, dengan fokus pada kontrol yang praktis.

No.	Lembaga	Peran Utama	Kerangka Kerja dan Panduan	Fokus pada Manajemen Kerentanan
9	ACSC	Otoritas keamanan siber Australia	▪ Peringatan keamanan ▪ Panduan teknis dan praktik terbaik	Fokus pada pertahanan nasional dan perlindungan infrastruktur kritis dengan pendekatan yang terkoordinasi untuk manajemen kerentanan.

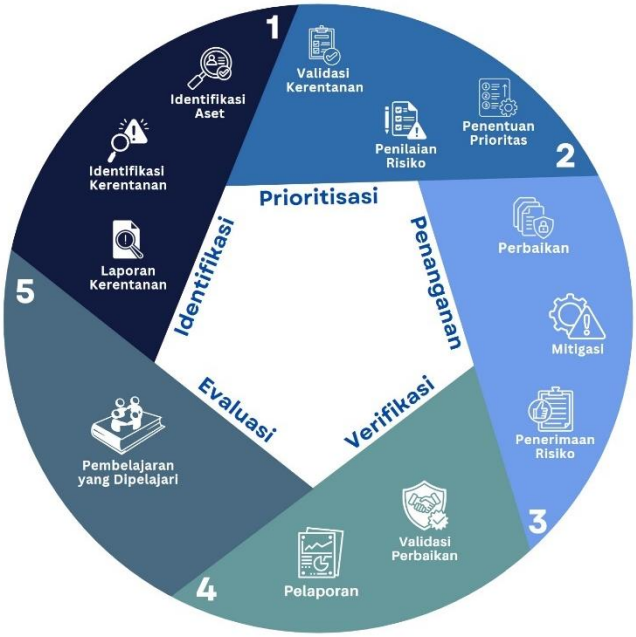
BAB V
SIKLUS MANAJEMEN KERENTANAN DI INDONESIA

It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it

- Stéphane Nappo

A. Gambaran Umum Program Manajemen Kerentanan

Manajemen kerentanan memiliki serangkaian proses yang melibatkan pemahaman mendalam tentang aset-aset penting dalam organisasi dan potensi ancaman terhadap aset tersebut. Tujuan utamanya adalah untuk mencegah eksploitasi kerentanan oleh pihak yang tidak berwenang, sehingga memastikan kelangsungan operasional dan perlindungan terhadap data sensitif organisasi.



Gambar 10. Siklus Manajemen Kerentanan

Manajemen kerentanan dapat dipandang sebagai sebuah siklus (Gartner, 2020). Artinya, manajemen kerentanan harus dilakukan secara berulang dan berkesinambungan secara teratur. Siklus Manajemen Kerentanan (dilihat pada Gambar 11) terdiri atas lima langkah utama yang berfungsi untuk memastikan sistem informasi organisasi tetap terlindungi dari ancaman keamanan.

Tahap pertama dalam siklus ini adalah identifikasi aset dan identifikasi kerentanan, yang mencakup proses inventarisasi terhadap aset-aset penting organisasi, seperti perangkat keras, perangkat lunak, jaringan, dan data yang harus dilindungi. Setelah itu, dilakukan pemindaian untuk mendeteksi kerentanan yang mungkin ada dalam sistem. Laporan kerentanan disusun berdasarkan hasil pemindaian dan sumber informasi lainnya, termasuk laporan dari pengguna atau peneliti eksternal.

Tahap kedua adalah prioritisasi kerentanan yang telah diidentifikasi. Proses ini dimulai dengan validasi kerentanan untuk memastikan bahwa temuan yang diperoleh relevan dan bukan *false positive*. Setelah itu, dilakukan penilaian risiko dengan mempertimbangkan dampak dan potensi eksploitasi dari setiap kerentanan. Berdasarkan hasil penilaian ini, organisasi menetapkan prioritas penanganan kerentanan, dengan fokus pada yang memiliki tingkat keparahan dan potensi dampak terbesar terhadap operasional bisnis.

Tahap ketiga dalam siklus ini adalah penanganan kerentanan, yang mencakup tindakan perbaikan, mitigasi, atau penerimaan risiko. Perbaikan dilakukan dengan cara menambal atau memperbarui sistem untuk mengatasi kerentanan yang ada. Jika perbaikan tidak dapat dilakukan secara langsung, mitigasi diimplementasikan untuk mengurangi dampak dari kerentanan tersebut. Dalam beberapa kasus, organisasi dapat memutuskan untuk menerima risiko tertentu jika dianggap bahwa dampaknya minimal atau biaya perbaikannya melebihi risiko yang ditimbulkan.

Tahap keempat adalah verifikasi terhadap tindakan penanganan yang telah diambil. Pada tahap ini, dilakukan validasi perbaikan melalui pengujian ulang terhadap kerentanan yang telah diperbaiki. Proses verifikasi ini juga mencakup pelaporan hasil untuk memastikan bahwa tindakan yang diambil telah berhasil mengatasi kerentanan dan sistem kembali aman.

Tahap kelima adalah evaluasi atas seluruh proses manajemen kerentanan. Organisasi meninjau efektivitas program manajemen

kerentanan dengan mengevaluasi langkah-langkah yang telah diambil, serta mendokumentasikan pembelajaran yang diperoleh. Evaluasi ini bertujuan untuk memperbaiki proses di masa mendatang dan memastikan siklus manajemen kerentanan terus beradaptasi dengan perubahan teknologi, ancaman baru, dan perkembangan dalam infrastruktur organisasi. Siklus ini berlangsung secara berkelanjutan sebagai bagian dari upaya menjaga keamanan sistem informasi organisasi.

B. Tahap Identifikasi

1. Identifikasi Aset

Sebelum melaksanakan rangkaian manajemen kerentanan, seluruh aset TI milik organisasi harus dapat diidentifikasi dengan baik. Identifikasi ini dapat dilakukan dengan mengumpulkan informasi-informasi yang relevan dari aset perangkat keras (*hardware*) dan perangkat lunak (*software*) (NIST, 2012). Identifikasi aset digunakan untuk mengetahui aset TI yang dimiliki oleh organisasi dan mengelompokkannya berdasarkan level prioritas dan kategorisasi tertentu sehingga dapat dijadikan sasaran manajemen kerentanan dengan tepat. Selain itu, dalam melakukan identifikasi aset, organisasi perlu memastikan bahwa informasi terkait identifikasi aset tersebut diperbarui secara berkala untuk mendapatkan daftar terbaru aset TI yang dimiliki organisasi.

Dalam proses manajemen kerentanan, langkah awal yang krusial adalah memastikan bahwa informasi yang dikumpulkan terkait aset TI hanya mencakup data yang relevan dan diperlukan. Informasi ini harus diidentifikasi, dikelompokkan, dan diprioritaskan untuk memfasilitasi pengelolaan kerentanan yang efektif. Rincian yang harus dikumpulkan meliputi nama sistem dan pengidentifikasi aset, nomor serial, serta informasi tentang pemilik dan administrator aset. Lokasi fisik aset dan detail mengenai *port* koneksi juga harus dicatat.

Selain itu, konfigurasi perangkat lunak dan perangkat keras dari setiap aset harus didokumentasikan dengan cermat. Untuk perangkat lunak, ini mencakup sistem operasi beserta nomor versinya, daftar aplikasi dan versi perangkat lunak, layanan jaringan yang aktif, serta alamat IP. Untuk perangkat keras, informasi yang relevan meliputi spesifikasi CPU, memori, ukuran penyimpanan, alamat *ethernet*, konfigurasi jaringan nirkabel, dan pengaturan I/O perangkat. Terakhir, versi *firmware* yang digunakan harus dicatat. Pengelompokan dan penentuan prioritas dari informasi ini akan membantu dalam penilaian dan mitigasi kerentanan yang lebih efektif, memungkinkan organisasi untuk menanggapi ancaman dengan lebih terstruktur dan tepat waktu.

Setelah dilakukan pengelompokan aset, maka dapat ditentukan level prioritas dari tiap aset TI. Penentuan level prioritas tersebut berguna untuk memetakan risiko yang terdapat pada tiap aset, mengetahui aset-aset yang membutuhkan perhatian khusus, dan menentukan pihak-pihak yang bertanggung jawab atas risiko awal yang muncul.

Dalam menentukan level prioritas aset, beberapa pertimbangan penting perlu diperhatikan untuk memastikan manajemen kerentanan yang efektif. Pertama, selera risiko organisasi menjadi faktor utama, yang mencerminkan tingkat risiko umum yang dapat diterima berdasarkan kebijakan dan strategi keamanan informasi organisasi. Selera risiko ini memberikan panduan tentang seberapa besar risiko yang bersedia diambil dan bagaimana hal tersebut memengaruhi prioritas pengelolaan aset.

Kedua, tingkat toleransi risiko organisasi juga berperan penting. Parameter ini menunjukkan tingkat risiko aset TI yang masih dapat diterima dan dikelola oleh organisasi tanpa mengganggu operasi atau keamanan. Toleransi risiko ini menentukan seberapa banyak risiko yang dapat dihadapi sebelum dianggap tidak dapat diterima dan memerlukan perhatian khusus.

Ketiga, mitigasi risiko yang dilakukan menunjukkan langkah-langkah yang telah diambil untuk menangani risiko awal yang

diidentifikasi pada aset TI. Termasuk di dalamnya kebijakan dan kontrol yang diterapkan untuk mengurangi atau mengelola risiko tersebut.

Penanganan risiko yang tersisa harus diperhitungkan setelah langkah mitigasi dilakukan. Hal ini mencakup risiko yang masih ada meskipun telah ada upaya mitigasi, dan memerlukan strategi tambahan untuk penanganan agar risiko tersebut tidak berdampak negatif pada organisasi. Dengan mempertimbangkan semua faktor ini, organisasi dapat menetapkan prioritas aset dengan lebih baik, memastikan sumber daya dialokasikan secara efektif untuk mengelola kerentanan yang paling kritis.

2. Identifikasi Kerentanan

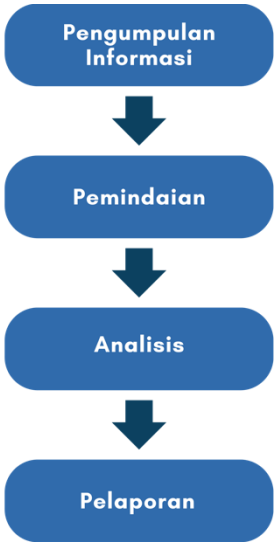
Pada bagian ini, dijelaskan mengenai definisi, metodologi, dan pelaporan dari *Vulnerability Assessment* (VA) dan *Penetration Testing* (PT) dalam tahap identifikasi pada Program Manajemen kerentanan di Indonesia.

a) *Vulnerability Assessment*

VA merupakan proses sistematis yang melibatkan identifikasi dan evaluasi kelemahan keamanan pada sistem informasi dengan membandingkan konfigurasi sistem tersebut dengan profil kerentanan yang telah diketahui sebelumnya (K. A. Scarfone et al., 2008). VA bisa dilakukan sebagai bagian dari proses PT atau sebagai proses yang berdiri sendiri dengan tujuan identifikasi kerentanan secara cepat pada jaringan, sistem, atau aplikasi tertentu. Tujuan dari VA adalah untuk menyediakan gambaran risiko keamanan untuk pengambilan langkah-langkah mitigasi sebelum kerentanan-kerentanan pada sistem dieksploitasi oleh pihak yang tidak berwenang.

Secara umum, proses VA melibatkan penggunaan mesin otomatis untuk melakukan pemindaian terhadap jaringan, sistem, dan aplikasi untuk mendeteksi potensi kerentanan seperti kesalahan konfigurasi atau perangkat lunak yang sudah usang. Secara umum, VA terdiri dari

beberapa proses yaitu pengumpulan informasi, pemindaian, analisis hasil, dan pelaporan seperti terlihat pada Gambar 12 (Sarker et al., 2023).



Gambar 11. Proses VA

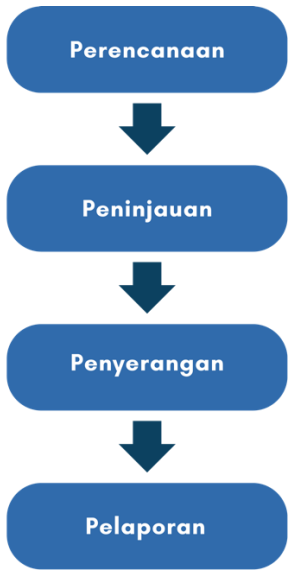
VA diawali dengan pengumpulan informasi yang diperlukan penguji untuk mengidentifikasi cakupan sistem, aplikasi, atau jaringan yang akan diuji (Goel & Mehtre, 2015; Sarker et al., 2023). Dari informasi yang didapatkan, dilakukan pemindaian terhadap target dengan tujuan mengidentifikasi kerentanan yang terdapat pada target. Hasil pemindaian kemudian dianalisis untuk menentukan tingkat prioritas dari kerentanan-kerentanan yang ditemukan untuk ditindaklanjuti. Langkah terakhir dalam proses VA adalah dokumentasi dan pelaporan.

b) *Penetration Testing*

PT adalah teknik pengujian keamanan pada aplikasi, sistem, atau jaringan dengan meniru serangan yang digunakan untuk mengeksploitasi suatu celah kerentanan (K. A. Scarfone et al., 2008). PT bertujuan untuk mengukur kemampuan sistem dalam menghadapi serangan dunia nyata dan menilai potensi kerugian akibat eksploitasi kerentanan. Oleh karena itu, PT harus direncanakan dengan baik dan

dilakukan oleh ahli untuk meminimalkan risiko kerugian selama pengujian.

Dalam melakukan PT, penguji dapat menggunakan beberapa strategi seperti *white box testing*, *black box testing*, dan *grey box testing* (Goel & Mehtre, 2015; Sarker et al., 2023). Perbedaan utama dari ketiga strategi ini terletak pada jumlah informasi yang diberikan oleh pemilik sistem kepada penguji. Pada *black box testing*, penguji tidak mendapatkan informasi apa pun mengenai target, sedangkan pada *white box testing*, penguji mendapatkan akses penuh ke informasi sistem. Sedangkan pada *Grey box testing* menggabungkan keduanya, yaitu penguji diberikan sebagian informasi tentang sistem yang akan diuji. Tahapan PT dapat dilihat pada Gambar 13.



Gambar 12. Tahapan *Penetration Testing*

Pengujian menggunakan PT diawali dengan fase perencanaan (K. A. Scarfone et al., 2008). Pada fase ini, ditentukan hal-hal mengenai rangkaian pengujian seperti cakupan target dan peraturan yang perlu disepakati. Hal ini untuk meminimalisir risiko yang bisa saja berdampak ke sistem target pengujian. Pada tahap ini, belum ada pengujian yang benar-benar dilakukan.

Fase selanjutnya dalam proses PT adalah fase peninjauan yang terdiri dari pengumpulan informasi dan pemindaian. Pengumpulan informasi dilakukan secara pasif maupun secara aktif. Pengumpulan informasi secara pasif berarti penguji mencoba mengumpulkan informasi-informasi yang sudah tersedia tanpa berinteraksi dengan sistem yang menjadi target pengujian. Sementara itu, pengumpulan informasi secara aktif melibatkan teknik-teknik yang dilakukan untuk mendeteksi kerentanan atau mendapatkan informasi dengan cara berinteraksi langsung dengan sistem target pengujian.

Fase penyerangan adalah inti dari PT. Informasi-informasi yang sudah dikumpulkan sebelumnya, disusun suatu rangkaian serangan untuk melakukan eksploitasi kerentanan sebagai verifikasi potensi kerentanan yang teridentifikasi. Jika eksploitasi berhasil dilakukan, maka kerentanan dianggap valid dan disusun langkah-langkah remediasi untuk menutup kerentanan tersebut. Beberapa teknik eksploitasi kerentanan membuat penguji dapat melakukan peningkatan hak akses pada sistem untuk mendapatkan lebih banyak informasi. Jika hal tersebut terjadi, maka diperlukan analisis lebih mendalam terkait tingkat risiko sebenarnya dari suatu kerentanan.

Fase pelaporan sebagai bagian dari PT merupakan fase terakhir. Dilakukan penyusunan laporan akhir dari hasil pengumpulan informasi hingga pengujian serangan terhadap sistem. Laporan akhir berisi mengenai kerentanan-kerentanan yang sudah divalidasi dan diberikan Langkah-langkah remediasi.

VA dan PT memiliki kelebihan dan kekurangan masing-masing dalam pengujian keamanan (Goel & Mehtre, 2015; Sarker et al., 2023; K. A. Scarfone et al., 2008). VA digunakan sebagai solusi untuk melakukan identifikasi kerentanan dengan cakupan yang luas dengan waktu yang relatif singkat. Sementara itu, PT digunakan untuk memvalidasi kerentanan teridentifikasi secara mendalam dan menilai dampak yang ditimbulkan jika kerentanan tersebut tereksploitasi. Meskipun memiliki kegunaan yang berbeda, hasil akhir berupa laporan VA maupun PT dapat

digunakan sebagai masukan proses identifikasi pada rangkaian proses Manajemen kerentanan.

3. Laporan Kerentanan

a) Call Center/ Pusat Bantuan

Penerimaan aduan siber, berupa temuan kerentanan memainkan peran penting dalam meminimalkan risiko serta memberikan informasi yang esensial untuk identifikasi dan pengelolaan kerentanan (National Cyber Security Centre, 2022). Pentingnya aduan kerentanan dapat meminimalkan risiko di antaranya:

1) Mengurangi Risiko Eksploitasi Kerentanan oleh Penyerang Tidak Beretika

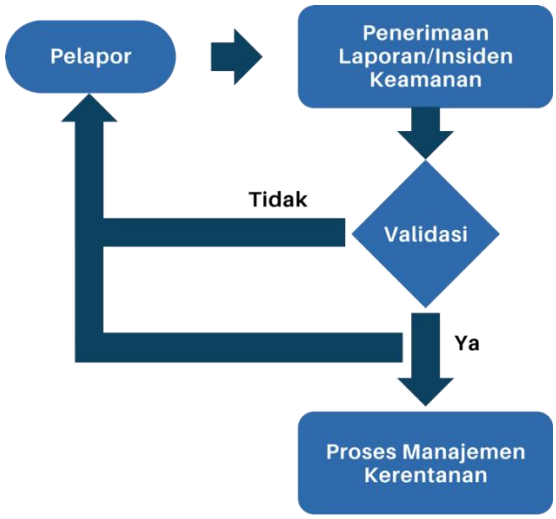
Penerimaan aduan siber dapat mengurangi jumlah kerentanan yang mungkin dieksploitasi oleh penyerang tidak beretika. Dengan demikian, risiko kerentanan ditemukan oleh pihak yang tidak bertanggung jawab dapat diminimalisir (National Cyber Security Centre, 2022).

2) Mencegah Dampak Publikasi Kerentanan oleh Penyerang

Tanpa adanya pusat aduan yang efektif, terdapat kemungkinan penyerang akan mempublikasikan kerentanan yang dapat merusak reputasi pemilik sistem. Oleh karena itu, penyediaan kontak pusat aduan sangat penting untuk memastikan adanya komunikasi yang efektif antara pelapor dan pemilik sistem (National Cyber Security Centre, 2022).

Kemampuan untuk menerima dan merespons aduan siber, baik dalam bentuk kerentanan maupun insiden sangat penting untuk memastikan keberlangsungan keamanan sistem. Aduan kerentanan dan insiden harus disalurkan ke titik kontak TTIS untuk segera ditindak lanjuti. Aduan siber yang diterima oleh CSIRT organisasi dapat langsung divalidasi dan dilakukan tindakan perbaikan. Sementara itu, aduan siber yang diterima oleh TTIS Nasional akan divalidasi sebelum diteruskan diteruskan ke TTIS Sektoral dan TTIS organisasi yang terdampak. Penempatan informasi kontak aduan berupa email ataupun nomor

telepon juga sangat penting, informasi terkait kontak aduan harus ditempatkan pada halaman web organisasi yang mudah ditemukan (BSSN, 2024). Proses pelaporan kerentanan dan insiden melalui pusat aduan diilustrasikan pada Gambar 13.



Gambar 13. Alur Proses Pelaporan Pusat Aduan
(BSSN (2024); IoT Security Foundation (2021))

Gambar 13 menunjukkan alur pelaporan insiden dan kerentanan melalui pusat aduan, yang berjalan berdasarkan diagram alur dengan input dan output yang jelas (IoT Security Foundation, 2021; Badan Siber dan Sandi Negara, 2024):

1) Pelapor: Entitas yang melaporkan insiden atau kerentanan terkait dengan sistem yang terdampak. Pelapor merupakan seorang individu, organisasi, amatir, profesional, pengguna akhir, peneliti keamanan, vendor, pemerintah atau pihak berkepentingan lainya.
2) Penerimaan Laporan Insiden/Kerentanan: Laporan yang diterima dari pelapor melalui pusat aduan yang tersedia pada sistem.
3) Validasi: Proses investigasi penyebab utama terjadinya insiden atau pengecekan kerentanan yang dilaporkan. Jika insiden atau kerentanan dianggap valid, laporan tersebut akan menjadi input dalam proses manajemen kerentanan dan dilanjutkan dengan komunikasi kepada pelapor. Sebaliknya, jika insiden atau kerentanan

dianggap tidak valid, laporan tersebut tidak dapat diterima dan akan dikomunikasikan kepada pelapor. Idealnya, komunikasi dengan pelapor harus berkelanjutan selama proses validasi berlangsung.

b) Vulnerability Disclosure Program

Berdasarkan data yang dihimpun oleh BSSN dalam rentang waktu 2020-2023, terdapat sebanyak 1436 laporan kerentanan yang diterima dari komunitas atau masyarakat umum. Fakta ini menunjukkan tingginya kontribusi publik dalam melaporkan temuan kerentanan pada sistem elektronik di Indonesia. Oleh karena itu, penting bagi organisasi untuk menyediakan jalur khusus yang efektif untuk menerima dan menindaklanjuti setiap laporan kerentanan yang masuk. Salah satu solusi yang dapat diterapkan adalah melalui penyelenggaraan program Pengungkapan Kerentanan *(Vulnerability Disclosure Program)*, yang memungkinkan partisipasi masyarakat dalam menjaga keamanan sistem organisasi secara proaktif.

Salah satu elemen terpenting dalam Program Pengungkapan Kerentanan adalah publikasi kebijakan yang jelas dan mudah diakses oleh semua pihak yang terlibat, termasuk pelapor dan pengguna sistem. Kebijakan ini harus mencakup cakupan kerentanan yang dapat dilaporkan, proses pelaporan yang harus diikuti, serta tindakan yang diharapkan dari organisasi dalam menanggapi laporan tersebut. Dengan mempublikasikan kebijakan secara transparan, organisasi dapat memperjelas ekspektasi dan mendorong pelapor untuk berpartisipasi secara aktif dan bertanggung jawab.

Menurut ISO/IEC 29147:2018(E) (ISO, 2018), organisasi perlu menetapkan kebijakan yang jelas dan transparan terkait proses pelaporan, penanganan, serta tindak lanjut laporan kerentanan. Tujuannya adalah untuk menyepakati maksud dan tujuan program serta menyamakan persepsi antara pelapor, pengguna, dan pemangku kepentingan lainnya.

Setiap organisasi dapat memiliki kebijakan yang berbeda sesuai dengan kebutuhan masing-masing. Kebijakan tersebut harus

menyatakan maksud organisasi, tanggung jawab, serta harapan terhadap pihak yang terlibat dalam program ini. Adapun hal-hal yang perlu dituangkan dalam kebijakan Program Pengungkapan Kerentanan menurut (ISO, 2018) adalah sebagai berikut:

1) Jalur Komunikasi

Setiap organisasi perlu menyertakan jalur komunikasi yang ditentukan bagi pelapor untuk mengirimkan detail kerentanan yang ditemukan. Jalur tersebut dapat berupa alamat e-mail, nomor telepon, formulir pada situs web, atau *customer service*.

- Alamat e-mail, contoh dari alamat email yang dapat digunakan untuk penerimaan laporan adalah sebagai berikut:
  - csirt@instansi.go.id
  - security@instansi.go.id
  - lapor-kerentanan@instansi.go.id
  - dan lainnya;
- Nomor telepon;
- Formulir pada situs web. Organisasi dapat menyediakan halaman khusus pada situs web, seperti situs CSIRT atau lainnya, yang berisi formulir pelaporan kerentanan. Langkah ini memudahkan pelapor dalam menyampaikan detail kerentanan sesuai dengan informasi yang telah ditentukan dalam formulir.
- *Customer service*, kontak *customer service* juga dapat digunakan untuk pelaporan kerentanan selama *customer service* telah dilatih untuk menerima laporan kerentanan.

2) Substansi Laporan

Organisasi perlu mencantumkan informasi apa saja yang dibutuhkan untuk memahami kerentanan yang ditemukan oleh pelapor. Substansi laporan harus mencakup informasi teknis yang lengkap dan relevan untuk membantu organisasi dalam memahami, mereproduksi, dan menilai kerentanan yang ditemukan. Laporan setidaknya mencakup deskripsi detail tentang kerentanan, sistem atau komponen yang terdampak, langkah-langkah untuk mereproduksi kerentanan, serta

potensi dampak atau risiko keamanan yang ditimbulkan. Selain itu, pelapor juga perlu menyertakan bukti *(proof-of-concept)* atau hasil eksploitasi untuk menunjukkan bahwa kerentanan tersebut valid.

Menurut Bugcrowd (2022), sebuah laporan kerentanan setidaknya memuat:

- Judul, memberikan gambaran singkat tentang jenis kerentanan yang ditemukan, lokasinya, serta dampaknya. Sebagai contoh, "*Remote File Inclusion* pada Formulir Unggah CV memungkinkan eksekusi kode jarak jauh";
- Target, sistem atau komponen atau situs yang terdampak oleh kerentanan tersebut, dapat berupa URL atau nama aplikasi;
- Tingkat kerentanan, tingkat kerentanan yang dihitung berdasarkan standar tertentu, seperti CVSS;
- Detail kerentanan, berisi informasi rinci mengenai kerentanan yang ditemukan. Mencakup penjelasan kerentanan, langkah-langkah eksploitasi, serta dampaknya.
- Lampiran, berisi bukti-bukti tambahan untuk melengkapi laporan, dapat berupa kode eksploitasi yang digunakan, tangkapan layar, rekaman layar dan sebagainya.

3) Opsi komunikasi yang aman

Dalam menerima laporan kerentanan, organisasi perlu memastikan komunikasi yang digunakan aman. Apabila jalur komunikasi yang digunakan menggunakan email, maka perlu disediakan *OpenPGP* untuk enkripsi email yang dikirimkan. Adapun bila jalur komunikasi menggunakan formulir pada situs web, maka perlu dipastikan situs web telah menerapkan TLS (HTTPS).

4) Standar Komunikasi

Di antara hal yang penting dalam penyelenggaraan Program Pengungkapan Kerentanan adalah memastikan komunikasi dengan pelapor terjalin dengan baik. Organisasi perlu menyampaikan standar komunikasi yang dapat diberikan, seperti memberikan respons awal, status terbaru serta pembaruan status dari kerentanan yang dilaporkan.

5) Cakupan

Organisasi perlu menyatakan cakupan yang termasuk dalam Program Pengungkapan Kerentanan. Cakupan ini merujuk pada batasan dan area spesifik yang termasuk dalam program pengungkapan kerentanan. Beberapa aspek cakupan yang dapat dijelaskan dalam kebijakan Program Pengungkapan Kerentanan, antara lain:

- Sistem dan Aplikasi yang tercakup, berisi daftar aplikasi yang termasuk ke dalam program. Dapat juga dibuat umum mencakup seluruh aset atau *subdomain* dari organisasi (misal *.instansi.go.id);
- Pengecualian, berisi daftar sistem atau aplikasi yang dikecualikan;
- Jenis kerentanan, berisi jenis kerentanan yang diharapkan untuk dilaporkan;
- Batasan aktivitas, berisi aktivitas yang tidak boleh dilakukan oleh pelapor, misalnya: melakukan social engineering, mempublikasi kerentanan tanpa seizin pemilik sistem, memanfaatkan kerentanan untuk eksploitasi lebih lanjut.

6) Penghargaan atau Pengakuan bagi pelapor

Di antara hal terpenting dalam penyelenggaraan Program Pengungkapan Kerentanan adalah bagaimana organisasi memberikan apresiasi terhadap pelapor yang telah membantu meningkatkan keamanan organisasi lewat kerentanan yang ditemukan. Penghargaan ini dapat berupa finansial, sertifikat, barang, pengakuan publik atau apresiasi lainnya sesuai dengan pertimbangan dari organisasi *Vendor Advisory*.

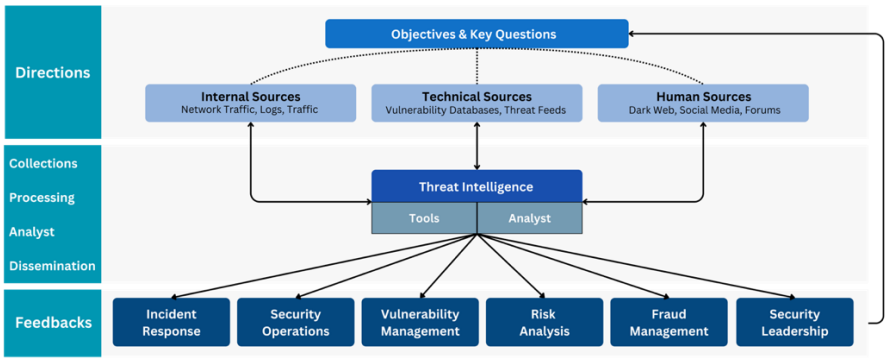
Laporan ini melibatkan penyediaan informasi resmi dari vendor perangkat lunak atau perangkat keras mengenai kerentanan yang ditemukan dalam produk mereka. *Vendor Advisory* biasanya mencakup deskripsi kerentanan, dampak yang mungkin terjadi, serta langkah-langkah mitigasi yang direkomendasikan, seperti penerapan *patch* atau perubahan konfigurasi. Informasi ini sangat penting bagi organisasi untuk memahami dan mengatasi kerentanan dengan cepat, sehingga dapat mengurangi risiko serangan siber. Vendor biasanya akan merilis

advisory setelah kerentanan diidentifikasi dan sebelum atau bersamaan dengan *patch* keamanan yang tersedia, sehingga pengguna dapat segera mengambil tindakan.

Dalam konteks manajemen kerentanan, *Vendor Advisory* membantu memastikan bahwa organisasi yang menggunakan produk tertentu mendapatkan informasi yang akurat dan tepat waktu untuk memitigasi risiko. Organisasi seperti Microsoft, Cisco, dan Oracle secara rutin merilis *Vendor Advisory* sebagai bagian dari tanggung jawab keamanan mereka. Selain itu, NIST dan CVE sering merujuk pada *Vendor Advisory* sebagai sumber resmi untuk memperbarui informasi kerentanan secara global (Booth et al., 2013; NIST, 2024).

c) Threat Intelligence Feeds

Threat intelligence merupakan rangkaian kegiatan dari mengumpulkan informasi hingga melakukan analisis untuk memahami ancaman siber yang mungkin menyerang sistem informasi atau jaringan komputer sehingga dapat menjadi masukan dalam pengambilan kebijakan keamanan organisasi (Knerler et al., 2022). Perkembangan teknologi yang pesat, kompleksitas jaringan komputer, dan beragamnya teknik yang digunakan oleh penyerang membuat proses identifikasi semakin sulit. Kegiatan *threat intelligence* berfokus untuk menemukan *threat actor* dan membedakannya dengan pengguna yang sah. Informasi yang dikumpulkan dari kegiatan *threat intelligence* dapat digunakan untuk identifikasi aktivitas penyerang dan tools yang digunakan dalam jaringan dan sistem elektronik.



Gambar 14. *Threat intelligence* Lifecycle[24]

Secara umum, *Cyber Threat intelligence* (CTI) memiliki 6 (enam) fase utama (Recorded Future, 2022) yang dikenal sebagai *Threat intelligence Lifecycle* sebagaimana disajikan pada Gambar 14. Penjelasan rincinya sebagai berikut:

1) *Direction*

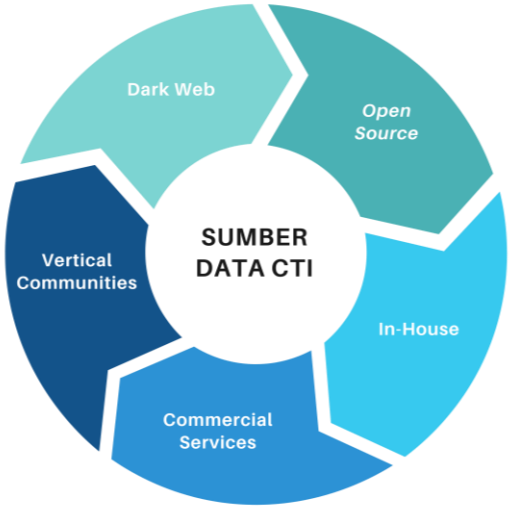
Fase ini adalah fase penetapan sasaran dan arah untuk kegiatan *threat intelligence*. Pada fase ini, pimpinan organisasi memiliki peran penting untuk menetapkan sasaran dan arah sesuai objektif yang ingin dituju oleh pemangku kepentingan dan pertanyaan permasalahan dalam menuju sasaran tersebut. Fase ini memerlukan pemahaman terhadap:

- Informasi aset dan proses bisnis yang perlu dilindungi.
- Potensi dampak dari terganggunya aset dan proses bisnis.
- Jenis informasi *threat intelligence* yang relevan dengan kepentingan *pemangku kepentingan*.
- Prioritas dalam perlindungan terhadap aset.

2) *Collection*

[24] https://www.recordedfuture.com/blog/threat-intelligence-lifecycle-phases

Fase ini merupakan fase pengumpulan informasi yang berguna untuk memberikan jawaban pertanyaan permasalahan. Informasi tersebut dapat berasal dari berbagai sumber yang dicari secara proaktif. Sumber-sumber informasi tersebut disajikan pada Gambar 15.



Gambar 15. Sumber informasi *threat intelligence* [25]

- *Open-Source Threat intelligence Feeds*

OSINT merupakan kegiatan pengumpulan informasi dari sumber terbuka seperti artikel, blog, media sosial, forum terbuka, dan sumber data publik lainnya. Sumber ini merupakan hasil kolaborasi penelitian banyak pihak dan selalu diperbarui secara berkala.

- *In-house Threat intelligence*

Sumber ini berasal dari hasil analisis internal yang dilakukan oleh organisasi berdasarkan pemantauan jaringan komputer internal. Informasi ini didapatkan oleh analis dari log *firewall*, IDS, dan perangkat jaringan lainnya.

- *Vertical Communities*

[25] https://www.recordedfuture.com/threat-intelligence-101/intelligence-sources-collection/threat-intelligence-sources

Dalam lingkungan tertentu, platform berbagi informasi siber dapat tersedia untuk komunitas yang sama, contohnya *Financial Services Information and Analysis Center* (FS-ISAC). FS-ISAC melibatkan beberapa industri perbankan di Amerika Serikat. Kelompok sejenis lainnya, seperti sektor industri dan sektor kesehatan, juga dapat memiliki saluran berbagi informasi serupa. Informasi *threat intelligence* juga dapat diperoleh melalui platform-platform berbagi informasi seperti ini.

- *Commercial Services*

Apabila *pemangku kepentingan* memiliki dukungan dari vendor keamanan terkait *threat intelligence*, maka informasi yang diberikan juga dapat dijadikan sebagai sumber informasi *threat intelligence*. Data yang bersumber dari vendor biasanya lebih komprehensif dan lebih minim adanya data *false-positive*. Namun, dalam penerapannya diperlukan adanya perbandingan secara terus menerus terhadap platform *threat intelligence* yang open-source seperti MISP agar mendapatkan komparasi informasi yang baik.

- *Dark Web Intelligence*

Dark Web merupakan bagian dari jaringan internet yang tidak dapat dilakukan pencarian secara normal. *Dark web* jamak digunakan untuk aktivitas yang ilegal dan dilarang. Dark web terdiri dari forum-forum digital yang bergerak secara *underground* dan memerlukan aplikasi khusus untuk mengaksesnya. Apabila dapat dilakukan *threat intelligence*, informasi rahasia seperti data yang diperjualbelikan, *malware* yang berkembang, dan aktivitas terlarang lainnya, informasi tersebut dapat digunakan sebagai sumber informasi *threat intelligence*.

3) *Processing*

Pada fase ini, dilakukan pemrosesan informasi yang dikumpulkan menjadi format yang dapat dimanfaatkan oleh pemangku kepentingan. Beragam data yang didapatkan dari proses *collection* merupakan data mentah sehingga harus dianalisis menggunakan *tools* tertentu atau dengan memanfaatkan analisis *threat intelligence*. Fase ini dapat

dilakukan dengan langkah-langkah seperti pengambilan alamat IP, mengekstrak data dari email, pengambilan sampel kebocoran data, pengambilan data aktivitas APT, *malware*, dan lain sebagainya. Fase *processing* juga dapat dilakukan berdasarkan *Indicator of Compromise* (IoC) sehingga dapat melakukan identifikasi informasi yang relevan sebagai data *threat intelligence*.

4) *Analysis*

Pada fase ini, dilakukan analisis informasi yang telah dikumpulkan dan disesuaikan dengan kebutuhan pemangku kepentingan menjadi informasi *threat intelligence* yang komprehensif sehingga dapat digunakan sebagai landasan dalam pengambilan keputusan. Analisis informasi ini harus relevan dengan pihak-pihak yang akan menggunakan data *threat intelligence* tersebut. Hasil analisis juga harus bersifat jelas dan dapat ditindaklanjuti.

5) *Dissemination*

Pada fase ini, hasil analisis informasi *threat intelligence* dibagikan dan disebarkan terhadap pihak-pihak yang membutuhkan. Pihak yang membutuhkan dapat berasal dari internal maupun eksternal pemangku kepentingan dan dapat digunakan untuk berbagai tujuan, salah satunya adalah sebagai masukan terhadap proses identifikasi kerentanan pada pelaksanaan manajemen kerentanan. Informasi yang diseminasikan dapat digunakan dalam proses identifikasi pada manajemen kerentanan seperti jenis dan penjelasan kerentanan yang dieksploitasi, risiko yang muncul dari aktivitas *threat actor*, dan lain sebagainya.

6) *Feedback*

Pada fase *feedback*, dilakukan respon secara interaktif terhadap aktivitas siklus *threat intelligence* yang dilakukan dari pihak-pihak pengguna informasi *threat intelligence*. Langkah ini diperlukan untuk terus memastikan informasi *threat intelligence* berguna dan tepat sasaran. Selain itu, juga untuk memastikan bahwa penerima merupakan

pihak yang dapat dipercaya untuk terus menerus menerima informasi dalam siklus *cyber threat intelligence*.

C. Tahap Prioritisasi

Proses prioritisasi dalam manajemen kerentanan merupakan elemen krusial dalam strategi keamanan siber organisasi. Langkah ini membantu menentukan kerentanan mana yang harus ditangani lebih dulu, dengan fokus pada mengelola risiko yang dapat merugikan operasional serta integritas sistem. Proses prioritisasi mencakup dua tahapan utama, yakni evaluasi dan penentuan prioritas. Evaluasi kerentanan bertujuan untuk memvalidasi keberadaan kerentanan yang telah teridentifikasi dan menilai potensi risiko yang dapat muncul jika kerentanan tersebut dieksploitasi. Tahapan ini mencakup analisis mendalam tentang dampaknya terhadap kerahasiaan, integritas, dan ketersediaan data serta sistem.

Setelah kerentanan dievaluasi, organisasi kemudian melakukan prioritisasi berdasarkan tingkat risiko yang diidentifikasi. Pendekatan ini memungkinkan organisasi untuk mengelola sumber daya secara efisien dengan memusatkan upaya mitigasi pada kerentanan yang paling kritis. Prioritisasi tidak hanya melihat aspek teknis, tetapi juga mempertimbangkan konteks bisnis, seperti aset yang paling berharga bagi organisasi, regulasi yang berlaku, dan ancaman aktif yang sedang terjadi. Dengan melakukan evaluasi risiko yang komprehensif, organisasi dapat mengurangi dampak eksploitasi potensial dan meningkatkan ketahanan sistem terhadap serangan siber.

Penetapan prioritas berdasarkan risiko memiliki peran vital dalam mencegah organisasi membuang sumber daya pada kerentanan yang berdampak minimal. Validasi yang cermat mengurangi risiko kesalahan dalam pengelolaan kerentanan, memastikan bahwa fokus mitigasi diarahkan kepada kerentanan yang benar-benar signifikan. Menggunakan kerangka kerja yang telah terbukti, seperti CVSS (FIRST, 2015) atau metodologi dari NIST SP 800-30 (NIST, 2012b), membantu

organisasi dalam proses pengambilan keputusan terkait urutan mitigasi yang paling efektif.

1. Validasi Kerentanan

Validasi adalah langkah pertama dalam proses evaluasi yang bertujuan untuk memastikan bahwa kerentanan yang telah diidentifikasi adalah benar dan relevan dengan lingkungan operasional organisasi. Validasi yang tepat meminimalkan risiko *false positives*, yang dapat mengarah pada penggunaan sumber daya yang tidak efisien.

Dalam proses validasi kerentanan, terdapat beberapa tahapan penting yang harus dilalui untuk memastikan efektivitas pengelolaan kerentanan. Pertama, proses validasi mencakup pengujian ulang kerentanan yang telah diidentifikasi dengan menggunakan berbagai alat yang berbeda serta konfirmasi manual oleh ahli keamanan siber. Uji coba eksploitasi di lingkungan terkendali sering kali diterapkan untuk memastikan apakah kerentanan tersebut dapat dieksploitasi. Pendekatan ini memungkinkan organisasi untuk memfokuskan sumber daya mereka hanya pada kerentanan yang benar-benar membawa risiko nyata terhadap sistem.

Kedua, beragam alat dan teknik tersedia untuk membantu proses validasi. Pemindai kerentanan otomatis, yang dapat dengan cepat mendeteksi kerentanan berdasarkan tanda-tanda yang ada dalam sistem, sering kali digunakan bersama dengan uji penetrasi manual yang dilakukan oleh tenaga ahli. Pemanfaatan kedua pendekatan ini secara bersamaan memberikan jaminan lebih baik bahwa kerentanan yang teridentifikasi adalah nyata dan relevan dengan kondisi sistem yang ada. Validasi ini memastikan bahwa organisasi dapat mengambil langkah mitigasi yang tepat dan sesuai dengan ancaman yang dihadapi.

Ketiga, terdapat beberapa tantangan signifikan dalam proses validasi kerentanan, salah satunya adalah hasil positif palsu yang sering kali mengganggu keakuratan analisis. Ketika data yang tidak lengkap atau tidak akurat digunakan dalam evaluasi, organisasi dapat salah

mengalokasikan sumber daya untuk mengatasi kerentanan yang sebenarnya tidak relevan. Oleh karena itu, diperlukan adanya tim ahli yang kompeten dan penggunaan alat validasi yang andal untuk meminimalkan risiko kesalahan dalam proses validasi. Organisasi yang mampu mengatasi tantangan ini dengan baik akan memiliki kemampuan yang lebih baik dalam mengelola risiko keamanan siber secara efektif.

2. Penilaian Risiko

Penilaian risiko adalah langkah kunci yang memungkinkan organisasi untuk memahami potensi dampak kerentanan terhadap operasi dan keamanan mereka. Penilaian ini terdiri dari analisis kritikalitas dan keparahan kerentanan yang telah divalidasi.

a) Komponen Penilaian Risiko

Penilaian risiko dalam keamanan siber adalah proses penting yang mencakup analisis mendalam terhadap berbagai komponen yang dapat mempengaruhi tingkat risiko suatu sistem atau jaringan. Salah satu komponen utama yang dinilai adalah kritikalitas, yang merujuk pada seberapa besar kemungkinan suatu kerentanan dapat dieksploitasi oleh pihak yang tidak berwenang. Kritikalitas ini mencakup analisis tentang tingkat kerentanan sistem, celah keamanan yang ada, serta peluang bagi penyerang untuk memanfaatkan celah tersebut. Sistem yang lebih sering diakses atau memiliki eksposur tinggi terhadap ancaman eksternal biasanya memiliki tingkat kritikalitas yang lebih tinggi.

Selain itu, penilaian juga mencakup keparahan atau dampak potensial yang dapat ditimbulkan apabila suatu kerentanan berhasil dieksploitasi. Keparahan ini diukur berdasarkan dampaknya terhadap tiga aspek utama keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan (CIA *Triad*). Dampak pada kerahasiaan bisa berarti hilangnya atau bocornya data sensitif, sementara dampak pada integritas bisa menyebabkan data dimodifikasi secara tidak sah, yang berpotensi merusak kepercayaan pada sistem. Terakhir, dampak

terhadap ketersediaan bisa menyebabkan gangguan layanan atau *downtime* yang signifikan, terutama jika sistem yang diserang merupakan bagian dari infrastruktur kritis.

Analisis kritikalitas dan keparahan secara menyeluruh, organisasi dapat memahami tingkat risiko yang dihadapi dan memprioritaskan upaya mitigasi berdasarkan tingkat ancaman yang paling mendesak. Hasil dari penilaian risiko ini membantu dalam pengambilan keputusan strategis terkait alokasi sumber daya dan penerapan kontrol keamanan yang lebih efektif, sehingga risiko keamanan siber dapat dikelola dengan lebih baik dan kerugian yang mungkin terjadi dapat diminimalkan.

b) Metodologi Penilaian Risiko

Metodologi yang digunakan dalam penilaian risiko bisa sangat beragam. Salah satu metode yang umum digunakan adalah CVSS (FIRST, 2015, 2017; Hanford & Heitman, 2015), yang memberikan skor berbasis metrik standar. Metodologi ini memungkinkan organisasi untuk mengevaluasi risiko dengan cara yang konsisten dan dapat dibandingkan.

Salah satu metodologi penilaian risiko adalah berbasis NIST SP 800-30. Pada tahap penilaian risiko dalam NIST SP 800-30 (NIST, 2012b), risiko yang telah diidentifikasi dievaluasi untuk menentukan tingkat risiko mereka, dengan mempertimbangkan dua parameter utama: kemungkinan terjadinya risiko dan dampaknya. Untuk penilaian kemungkinan terjadinya risiko, dilakukan pengukuran probabilitas untuk menilai seberapa mungkin ancaman tertentu dapat mengeksploitasi kerentanan yang ada, menggunakan data historis, pengalaman sebelumnya, atau analisis tren. Biasanya, penilaian ini menggunakan skala deskriptif seperti "tidak mungkin", "kemungkinan rendah", "kemungkinan sedang", "kemungkinan tinggi", atau "pasti", untuk memberikan gambaran frekuensi terjadinya risiko. Evaluasi situasional juga penting, mengingat faktor-faktor seperti lingkungan operasional dan keamanan fisik yang dapat mempengaruhi kemungkinan risiko.

Untuk penilaian dampak risiko, langkah ini mencakup pengukuran seberapa besar kerugian atau dampak yang mungkin terjadi jika risiko terwujud, seperti kerugian finansial, kerusakan reputasi, atau dampak operasional. Skala deskriptif digunakan untuk menggambarkan dampak potensial dengan kategori seperti "rendah", "sedang", "tinggi", atau "kritikal". Selain itu, analisis konsekuensi dilakukan untuk menilai efek jangka pendek dan jangka panjang dari dampak risiko terhadap aset, operasi, dan tujuan organisasi. Dalam kombinasi kemungkinan dan dampak, penilaian ini menggabungkan kedua parameter untuk menentukan tingkat risiko secara keseluruhan, sering kali dengan menggunakan matriks risiko yang menghubungkan probabilitas dengan dampak. Kategorisasi risiko membantu dalam memprioritaskan risiko yang harus ditangani terlebih dahulu, seperti dalam kategori "tinggi", "sedang", atau "rendah". Metodologi penilaian dapat bersifat kualitatif, menggunakan penilaian subjektif berdasarkan pengetahuan dan pengalaman, atau kuantitatif, menggunakan data numerik dan teknik statistik untuk memberikan estimasi yang lebih terukur. Dokumentasi hasil penilaian risiko, termasuk metode yang digunakan, penting untuk referensi di masa depan dan kepatuhan, sedangkan pelaporan menyajikan hasil secara jelas untuk mendukung pengambilan keputusan terkait mitigasi risiko.

c) Dampak Penilaian Risiko yang Tidak Tepat

Penilaian risiko yang akurat dan konsisten adalah elemen kunci dalam manajemen kerentanan yang efektif. Kegagalan dalam melakukan penilaian risiko yang tepat dapat mengakibatkan konsekuensi yang serius, seperti serangan siber yang merugikan dan alokasi sumber daya yang tidak efisien. Kesalahan dalam penilaian dapat menyebabkan organisasi mengalokasikan terlalu banyak atau terlalu sedikit sumber daya untuk ancaman tertentu, yang pada gilirannya dapat mengganggu keseluruhan keamanan siber.

Untuk menghindari hal ini, sangat penting bagi organisasi untuk mengembangkan dan menerapkan metodologi penilaian risiko yang

dapat diandalkan dan teruji. Metodologi ini harus mencakup identifikasi aset, penilaian kerentanan, dan evaluasi potensi dampak yang dapat ditimbulkan oleh setiap kerentanan. Selain itu, penting juga untuk memperhatikan konteks bisnis, termasuk aspek hukum dan kepatuhan serta pertimbangan biaya dan manfaat dari tindakan pengamanan yang diambil.

Menurut Chaudhary et al. (2022), penilaian risiko yang efektif tidak hanya mengurangi kemungkinan serangan siber, tetapi juga meningkatkan efisiensi operasional dengan mengarahkan sumber daya ke area yang paling membutuhkan. Oleh karena itu, implementasi kerangka kerja penilaian risiko yang komprehensif, seperti yang direkomendasikan oleh NIST atau ISO 27005, sangat dianjurkan.

Chen (2021) menegaskan bahwa pendekatan sistematis terhadap penilaian risiko dapat memperkuat kemampuan organisasi dalam mengidentifikasi dan mengurangi risiko keamanan siber secara efektif. Penelitian ini juga menekankan pentingnya pelatihan reguler dan pembangunan kapasitas sebagai bagian dari proses manajemen risiko untuk memastikan semua pihak yang terlibat memahami risiko dan tanggapan yang tepat terhadapnya.

3. Prioritisasi Kerentanan

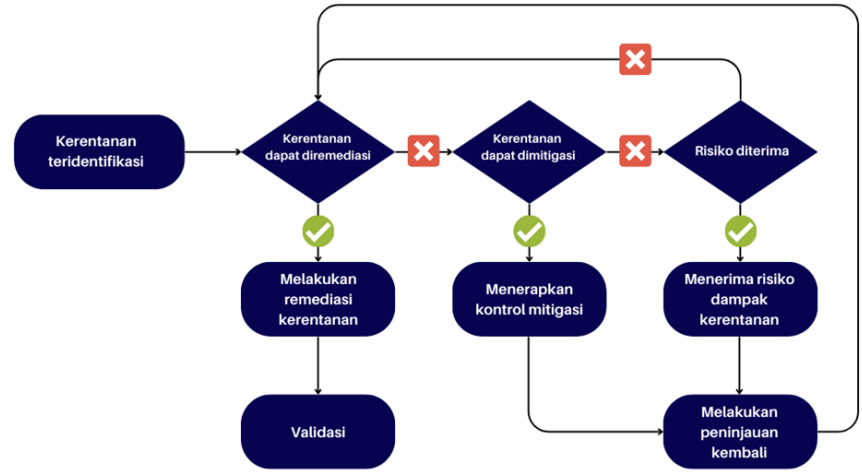
Setelah risiko dinilai, tahap berikutnya adalah menetapkan prioritas untuk tindakan remediasi dengan mempertimbangkan konteks spesifik yang mempengaruhi pentingnya setiap kerentanan[26]. Pada tahap penilaian konteks, beberapa faktor kunci dipertimbangkan untuk menentukan prioritas kerentanan. Nilai aset menjadi salah satu faktor utama, pada kondisi ini aset yang terkena dampak kerentanan dievaluasi berdasarkan nilainya bagi organisasi. Kerentanan yang mempengaruhi aset yang sangat berharga—seperti data sensitif atau sistem kritikal—

[26]https://www.isaca.org/resources/news-and-trends/industry-news/2023/using-a-risk-based-approach-to-prioritize-vulnerability-remediation

mendapatkan prioritas lebih tinggi karena dampak potensialnya terhadap operasi dan keamanan organisasi. Kepatuhan dan regulasi juga memainkan peran penting, karena kerentanan yang terkait dengan kewajiban kepatuhan atau regulasi yang harus dipatuhi organisasi mungkin mendapatkan prioritas lebih tinggi untuk menghindari sanksi hukum dan kerugian reputasi. Ancaman aktif adalah faktor tambahan yang dipertimbangkan, karena kerentanan yang sedang menjadi target serangan aktif harus diprioritaskan untuk mitigasi segera. Berdasarkan hasil evaluasi dan penilaian konteks, penetapan prioritas dilakukan dengan dua metode utama: Matriks prioritas, yang menggabungkan penilaian dampak dan kemungkinan eksploitasi untuk menentukan tingkat risiko secara keseluruhan, dan Kategorisasi risiko, dalam hal ini kerentanan dikelompokkan dalam kategori prioritas seperti "tinggi", "sedang", atau "rendah" untuk merencanakan mitigasi dan mengalokasikan sumber daya secara efektif.

D.Tahap Penanganan

Penanganan terhadap kerentanan yang ditemukan harus dilakukan organisasi untuk menjaga aset Organisasi dari serangan dan ancaman yang mungkin muncul dari kerentanan tersebut. Secara garis besar proses penanganan kerentanan yang dilakukan Organisasi dapat dilakukan melalui tahapan remediasi, mitigasi, dan penerimaan kerentanan. Alur proses tersebut dapat dilihat pada Gambar 16.



Gambar 16. Tahapan Penanganan Kerentanan (Gartner, 2020)

1. Remediasi

Berdasarkan ISO/IEC 30111:2019(E) (ISO, 2019), organisasi perlu melakukan remediasi yang terbagi ke dalam 3 tahap:

a) Menentukan keputusan remediasi

Pada tahap ini organisasi perlu menentukan remediasi seperti apa yang dapat dilakukan. Beberapa pertimbangan yang perlu diperhatikan:

1) Kecepatan remediasi, pada dasarnya kerentanan perlu diremediasi dengan cepat, terutama kerentanan dengan tingkat risiko tinggi atau kritikal. Namun organisasi juga perlu memastikan langkah remediasi yang dilakukan dapat menutup kerentanan dengan baik.
2) Pengujian, remediasi yang dilakukan perlu diuji untuk memastikan tidak menimbulkan masalah baru atau berdampak negatif bagi sistem.
3) Tingkat risiko eksploitasi, organisasi perlu memperhatikan tingkat risiko eksploitasi dari kerentanan, termasuk apabila kerentanan tersebut mudah dieksploitasi atau telah berhasil dieksploitasi secara publik.

4) Solusi sementara, dalam hal kerentanan memiliki risiko yang tinggi, solusi sementara dapat dilakukan untuk mencegah kerentanan dieksploitasi secara masif, hingga terdapat remediasi utuh yang dapat menutup kerentanan dengan komprehensif.

b) Melakukan remediasi

Remediasi kerentanan merupakan langkah kritikal dalam manajemen kerentanan yang efektif (Government of South Australia, 2021). Organisasi harus melaksanakan strategi remediasi yang telah diputuskan, yang bisa mencakup berbagai tindakan seperti membuat (K. Scarfone & Souppaya, 2022), melakukan pembaruan, memperbaiki kode sumber, atau melakukan perubahan konfigurasi untuk menutup kerentanan yang teridentifikasi. Tindakan ini dirancang untuk memperkuat sistem terhadap serangan potensial dan mengurangi risiko keamanan yang dihadapi.

c) Menguji hasil remediasi

Organisasi perlu memastikan dan menguji tindakan remediasi yang sudah dilakukan dapat menutup kerentanan. Serta perlu dipastikan tidak menimbulkan kerentanan baru, atau masalah lain yang mengganggu operasional sistem. Jika ditemukan adanya permasalahan yang ditimbulkan, maka organisasi perlu memperbarui atau mengubah remediasi yang telah dilakukan.

Proses remediasi perlu segera dilakukan sesuai dengan hasil analisis, perhitungan tingkat kerentanan dan prioritisasi (University of Toronto, 2024). Dalam hal organisasi tidak dapat menyelesaikan remediasi sesuai jangka waktu yang direkomendasikan di atas, maka perlu dilakukan langkah mitigasi untuk memperkecil tingkat *likelihood* dari suatu kerentanan.

2. Mitigasi

Mitigasi adalah tahapan kedua dalam tahapan tindakan manajemen kerentanan. Upaya mitigasi harus dilakukan oleh organisasi jika kerentanan tidak dapat diremediasi secara penuh oleh organisasi. Beberapa kondisi dan alasan yang dapat menjadi penyebab mitigasi harus dilakukan adalah jika langkah remediasi yang diperlukan dapat mengganggu berjalannya proses bisnis aplikasi, keterbatasan teknologi yang membutuhkan biaya, dan belum adanya *update/patch* yang disediakan oleh vendor teknologi terdampak[27].

Tim manajemen kerentanan yang menemukan/mengetahui kerentanan pada organisasi tidak selalu bertanggung jawab untuk melakukan perbaikan dan melaksanakan langkah mitigasi atau memberikan solusi dari kerentanan tersebut. Namun, Tim VM harus memberikan informasi dan berkoordinasi dengan pemangku kepentingan/bagian terkait.

Terdapat 3 (tiga) model mitigasi kerentanan (Roytman & Bellis, 2023) yang dapat diterapkan oleh organisasi sesuai dengan kebutuhan:

1) *Asset-Centric*: Fokus kepada dampak terhadap proses bisnis, nilai organisasi, dan nilai aset, dengan pendekatan pengurangan risiko secara bertahap.
2) *Vulnerability Centric*: Fokus kepada kemungkinan terjadi dan dampak dari kerentanan, dengan pendekatan risiko secara bertahap.
3) *Threat Centric*: Fokus pada kerentanan yang sering kali menjadi target aktivitas *malware*, *ransomware*, dan *threat actors*, dengan pendekatan pengurangan risiko secara bertahap.

Upaya mitigasi dilakukan untuk meminimalkan risiko yang dapat diakibatkan dari kerentanan tersebut, sehingga keberlangsungan proses bisnis organisasi dapat tetap berjalan secara normal. Untuk melakukan upaya mitigasi, organisasi disarankan membuat rencana mitigasi kerentanan yang setidaknya meliputi namun tidak terbatas pada[28]:

[27]https://www.rapid7.com/blog/post/2020/09/14/vulnerability-remediation-vs-mitigation-whats-the-difference/).

[28] https://www.esecurityplanet.com/compliance/vulnerability-management-policy-template/

a) Penerapan kontrol keamanan untuk mitigasi kerentanan

Penerapan perangkat lunak/*tools* keamanan dapat menjadi alternatif untuk melakukan mitigasi berupa deteksi, proteksi, dan analisis keamanan secara efektif. Beberapa perangkat lunak/tools yang dapat diterapkan sebagai mitigasi kerentanan antara lain adalah *Security Information and Event Management* (SIEM), *Endpoint Detection and Response* (EDR), *Next-Generation Firewalls* (NGFW), *Antivirus/Anti-Malware*, *Patch Management Systems* (Deputi III, 2024).

b) Penerapan multi-factor authentication (MFA)

Penerapan MFA dapat dilakukan ketika diketahui kerentanan yang bersumber dari adanya penggunaan mekanisme autentikasi yang kurang tepat atau kerentanan itu berasal dari fitur aplikasi yang berada pada sisi pengguna (Mohammed et al., 2023).

c) Pengisolasian sumber daya/perangkat yang rentan

Pengisolasian sumber daya/perangkat yang rentan dilakukan sebagai langkah sementara ketika *patching* belum dapat dilakukan pada sumber daya/perangkat yang rentan. Langkah ini dapat dilakukan dengan pemblokiran akses, segmentasi jaringan, hingga pengisolasian sistem. Langkah ini dilakukan untuk mencegah adanya akses tidak sah terhadap sumber daya/perangkat yang rentan (Government of South Australia, 2021).

d) Penghapusan atau penghentian penggunaan sumber daya/perangkat yang rentan

Penghapusan atau penggantian sumber daya/perangkat yang rentan dilakukan sebagai tindak lanjut ketika sumber daya/perangkat tidak dapat diisolasi dan dilindungi lagi, sehingga untuk mengantisipasi adanya eksploitasi oleh pihak tidak bertanggung jawab maka perlu dilakukan penghapusan atau penghentian penggunaan sumber daya/perangkat tersebut.

e) Peningkatan atau penggantian sumber daya/perangkat yang rentan

Peningkatan atau penggantian sumber daya/perangkat yang rentan dilakukan sebagai langkah lanjutan ketika terdapat kerentanan yang tidak dapat diremediasi namun Organisasi memiliki ketergantungan terhadap sumber daya/perangkat terkait, sehingga perlu dilakukan penyesuaian dengan melakukan peningkatan/*upgrade* dari sumber daya/perangkat tersebut atau dengan melakukan penggantian sumber daya/perangkat yang memiliki fungsi serupa, sehingga proses bisnis dari Organisasi dapat tetap berjalan.

Rencana mitigasi kerentanan dapat digunakan oleh organisasi ketika ditemukan sebuah kerentanan yang tidak dapat diremediasi secara langsung. Untuk menerapkan langkah mitigasi, organisasi harus melakukan percobaan pada sistem skala kecil guna mengetahui kompabilitas dari langkah mitigasi yang dilakukan terhadap sistem, sehingga tidak mengganggu operasional proses bisnis yang berjalan ketika diterapkan dalam sistem besar (K. Scarfone & Souppaya, 2022). Dalam hal remediasi dan mitigasi tidak dapat dilakukan oleh organisasi, maka organisasi harus menerima risiko dan dampak yang mungkin terjadi dari kerentanan yang diketahui.

3. Penerimaan Risiko

Penerimaan terhadap risiko dilakukan sebagai langkah terakhir dalam penanganan kerentanan. Pada tahap ini organisasi harus menentukan apakah risiko dari kerentanan tersebut dapat diterima oleh organisasi atau tidak. Jika risiko dari kerentanan tidak dapat diterima, maka organisasi harus kembali ke tahap remediasi dan menentukan cara yang dapat dilakukan untuk memperbaiki kerentanan tersebut atau melakukan mitigasi untuk mengurangi risiko dari kerentanan tersebut. Jika risiko dari kerentanan berada pada level yang dapat diterima oleh organisasi tanpa dilakukan remediasi dan mitigasi, maka dampak yang

mungkin terjadi dari risiko kerentanan tersebut menjadi tanggung jawab organisasi.

E. Tahap Verifikasi

1. Validasi Perbaikan

Setelah proses remediasi atau mitigasi dilakukan, perlu pengujian kembali kerentanan yang ditemukan melalui kegiatan validasi. Validasi perbaikan bertujuan untuk memastikan bahwa kerentanan sudah berhasil ditangani dan tidak menimbulkan masalah baru (ISO, 2019). Ketika melakukan validasi ternyata perbaikan gagal, maka tahapan remediasi atau mitigasi harus diulang kembali.

2. Pelaporan

Pelaporan adalah salah satu komponen penting dari rangkaian proses manajemen kerentanan. Pemanfaatan manajemen kerentanan dapat memberikan beragam jenis laporan sesuai dengan kebutuhan penerima laporan. Dalam sebuah laporan dapat berisikan penjelasan data-data yang terkandung dalam laporan, bagaimana nilai-nilai data pada laporan diperoleh atau dihitung dan pendefinisian pengguna yang menggunakan laporan (Kissoon, 2022). Dalam pelaporan, Tim CSIRT menganalisis dan menginterpretasikan data tentang kerentanan terbaru yang ditemukan. Data tersebut dilaporkan untuk digunakan dalam pengambilan keputusan strategis. Laporan ini memuat informasi terkait nama kerentanan, waktu ditemukannya kerentanan, deskripsi terkait kerentanan, remediasi dan tindak lanjut yang sudah dilakukan dan tujuan penerima laporan dengan cara dan format yang dapat dipahami (FIRST, 2023).

Dalam langkah pelaporan, pengiriman laporan dilakukan kepada pihak terkait baik dalam internal organisasi dan pihak eksternal yang terkena dampak kerentanan tersebut. Pihak internal organisasi

utamanya ditujukan kepada pimpinan organisasi dan dilakukan sesegera mungkin setelah kerentanan ditemukan. Selain itu, laporan juga dapat dikirimkan terhadap pihak eksternal sebagai berikut (Guidelines for Cyber Security Incidents, 2024):

a) Laporan kepada CSIRT Nasional

BSSN sebagai CSIRT Nasional memiliki kanal aduan siber untuk menerima laporan kerentanan dan memberikan asistensi penanganan kerentanan. CSIRT sektoral dan/atau CSIRT organisasi dihimbau untuk melakukan koordinasi terkait laporan tersebut kepada BSSN. Laporan ini juga digunakan oleh BSSN untuk mengidentifikasi dan menganalisis tren kerentanan yang terdapat di Indonesia.

b) Laporan kepada *customer* dan publik

Pelaporan kerentanan kepada *customer* dan publik dalam kurun waktu tertentu setelah ditemukan kerentanan menunjukkan komitmen organisasi terhadap penanganan kerentanan tersebut. Kerentanan yang menyangkut perangkat keras, perangkat lunak, maupun informasi terkait *customer* dan publik harus segera dilaporkan untuk dapat dilakukan tindak lanjut terhadap pihak yang terdampak.

CSIRT dihimbau untuk dapat berbagi informasi dengan organisasi lain dengan aman [29]. Proses pengiriman laporan memerlukan saluran komunikasi yang aman untuk menjamin aspek kerahasiaan, integritas, autentikasi, dan nirsangkal. Selain itu, proses pengiriman laporan juga harus mempertimbangkan kebijakan keamanan organisasi yang berlaku. Saluran komunikasi yang digunakan disesuaikan dengan kebutuhan organisasi dan pemilik sistem. Semua informasi yang didistribusikan harus diberi klasifikasi informasi sesuai dengan kebijakan berbagi informasi.

[29] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1 :: 6.5

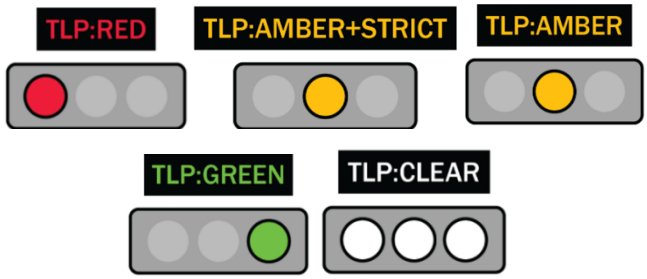
Pengguna laporan ditentukan berdasarkan tahap identifikasi yang terdiri dari identifikasi kerentanan (VA/PT) dan laporan kerentanan (*Call Center*, *Vulnerability Disclosure Program*, *Vendor Advisory* dan *Threat Inteligence Feeds*) sebagaimana digambrkan dalam tabel 3.

Tabel 3. Penerima laporan

No.	Identifikasi VM	Feedback Laporan	Keterangan
1	VA/PT	Pelaksana VA/PT	Laporan yang dikirimkan merupakan validasi atas temuan kerentanan dan remediasi terhadap kerentanan yang ditemukan.
2	Call Center/VDP	Pelapor	Laporan yang dikirimkan merupakan validasi atas temuan kerentanan dan pemberian reward atau bounty
3	*Vendor Advisory*	Pemilik Sistem dan eksternal terdampak	Laporan ditujukan terhadap organisasi atau individu yang memiliki kesamaan aset terdampak
4	Cyber Threats Inteligence Feeds	Pemilik Sistem	Laporan ditujukan terhadap organisasi atau individu yang memiliki kesamaan aset terdampak

Klasifikasi informasi laporan mengacu pada konsep *Traffic Light Protocol* (TLP). TLP merupakan standar klasifikasi informasi yang dikeluarkan oleh FIRST (CISA, 2024). TLP ini digunakan untuk memfasilitasi pembagian informasi sensitif agar dapat didistribusikan dan dimanfaatkan secara tepat dan aman. TLP memiliki 4 (empat) label yaitu TLP:RED, TLP:AMBER+STRICT, TLP:AMBER, TLP:GREEN, dan TLP:CLEAR[30].

[30] https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage



Gambar 17. Traffic Light Protocol (TLP)

1) TLP:RED

TLP ini digunakan untuk laporan yang memerlukan tindak lanjut dengan informasi sangat sensitif, seperti yang berkaitan dengan privasi, reputasi, atau proses bisnis organisasi. Laporan dengan klasifikasi TLP ini hanya boleh disampaikan kepada penerima yang dituju.

2) TLP:AMBER+STRICT

TLP ini diterapkan pada laporan yang memerlukan tindak lanjut dengan informasi yang berisiko terhadap privasi, reputasi, dan proses bisnis organisasi jika dibagikan di luar organisasi. TLP ini umumnya digunakan untuk kebutuhan internal organisasi guna mendukung operasional dan kepentingan organisasi tersebut.

3) TLP:AMBER

TLP ini diberlakukan untuk laporan yang memerlukan tindak lanjut dengan informasi yang menimbulkan risiko terkait privasi, reputasi, dan proses bisnis organisasi jika dibagikan di luar organisasi dan kepada klien lain yang terkait dengan organisasi. TLP ini biasanya digunakan untuk internal organisasi dan klien terkait untuk mencegah dampak yang lebih meluas.

4) TLP:GREEN

TLP ini dipakai untuk laporan yang berguna dalam rangka peningkatan kesadaran keamanan dalam suatu komunitas. TLP ini dapat

digunakan untuk berbagi informasi antar organisasi dalam komunitas yang sama namun dibagikan melalui saluran komunikasi tertentu.

5) TLP:CLEAR

TLP ini digunakan untuk laporan yang tidak mengandung informasi sensitif dan dapat didistribusikan sesuai prosedur publik. Dokumen dengan TLP ini dapat disebarluaskan secara bebas tanpa pembatasan khusus.

F. Tahap Evaluasi

Tahap evaluasi dalam bertujuan sebagai sarana pengembangan berkelanjutan. Pada tahap ini, organisasi mengevaluasi tindakan-tindakan yang telah dilakukan untuk menilai proses yang diselenggarakan. Dalam pelaksanaan evaluasi manajemen kerentanan pada organisasi, tim tanggap insiden siber dapat menerapkan beberapa langkah seperti berikut:

1. Menentukan strategi evaluasi yang akan digunakan pada organisasi.

   Beberapa metode seperti SAW dan WPM (Pipyros, 2019), dapat dimanfaatkan sebagai strategi organisasi dalam melakukan evaluasi dengan mempertimbangkan situasi dan kondisi.

2. Identifikasi tujuan dan hasil dari manajemen kerentanan yang telah dilakukan.

   Dari hasil identifikasi kedua aspek tersebut, dapat dilakukan analisis efektivitas proses manajemen kerentanan yang telah dilakukan sehingga proses evaluasi berjalan secara efisien.

3. Menentukan matriks evaluasi (Swanagan, 2024).

   Matriks evaluasi diperlukan sebagai sarana konsistensi dalam melakukan evaluasi berkelanjutan. Dengan adanya matriks yang telah ditetapkan, organisasi lebih mudah mengomunikasikan hasil evaluasi dalam menjalankan manajemen kerentanan.

4. Melakukan kolaborasi dan *benchmarking* dengan tim tanggap insiden siber organisasi lain.

Benchmarking dapat dimanfaatkan sebagai sarana pembelajaran dan peningkatan kapasitas suatu organisasi. Dengan adanya *benchmarking*, organisasi mengetahui apa yang menjadi kekurangan dan bisa memetik pembelajaran dari pihak lain.

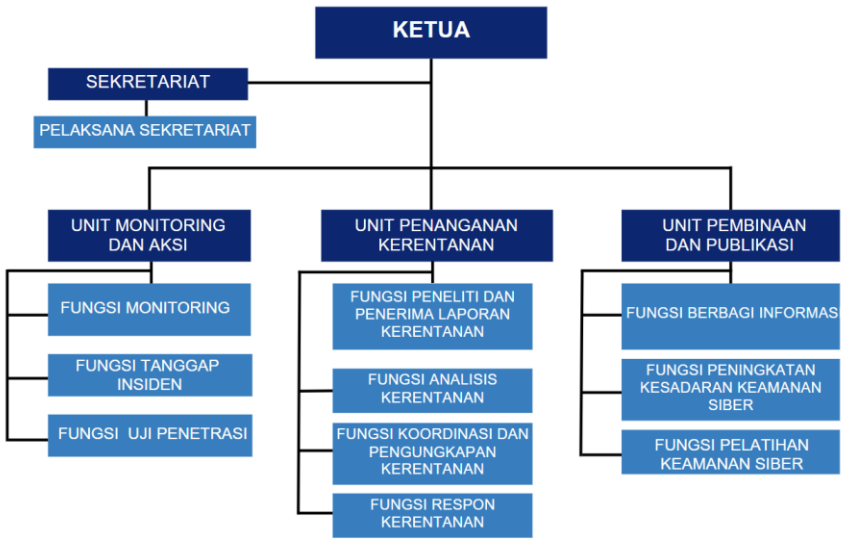
BAB VI

STRATEGI PENERAPAN MANAJEMEN KERENTANAN PADA ORGANISASI

Privacy is not an option, and it shouldn't be the price we accept for just getting on the internet.

- Gary Kovacs

Penerapan Manajemen Kerentanan pada organisasi perlu dilakukan secara efektif dan efisien. Manajemen Kerentanan dapat diampu oleh TTIS organisasi atau unit lain yang menangani fungsi keamanan siber pada organisasi. Bagian ini menjelaskan terkait langkah-langkah implementatif siklus manajemen kerentanan pada organisasi khususnya pada TTIS organisasi. Berdasarkan Peraturan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia Nomor 1 Tahun 2024 tentang Pedoman Pembentukan Tim Tanggap Insiden Siber Sektor Pemerintahan, struktur TTIS secara umum dengan merujuk pada TTIS sektor pemerintahan dalam Gambar 18.



Gambar 18. Struktur organisasi mengacu pada TTIS sektor pemerintahan

Berdasarkan struktur tersebut, TTIS dipimpin oleh Ketua dan didampingi oleh sekretariat. Terdapat 3 (tiga) unit pelaksana TTIS yaitu Unit Monitoring dan Aksi, Unit Penanganan Kerentanan, dan Unit Pembinaan dan Publikasi. Seluruh unit memiliki perannya masing-masing dalam pelaksanaan pengelolaan kerentanan organisasi.

Langkah-langkah dalam penerapan manajemen kerentanan pada TTIS organisasi dijelaskan sebagai berikut.

A. Tahap Identifikasi

1. Identifikasi Aset

Langkah identifikasi pertama yang harus dilakukan TTIS adalah melakukan identifikasi aset yang dimiliki. Identifikasi aset dapat dilakukan dengan langkah-langkah sebagai berikut:

a) Menyusun kebijakan terkait proses identifikasi aset.
b) Menyusun *risk register* aset yang dimiliki.
c) Melakukan identifikasi aset perangkat keras dan perangkat lunak. Informasi yang dikumpulkan merupakan informasi yang relevan untuk digunakan seperti:
   - Aset internal dan eksternal;
   - Lingkungan aset yang bersifat *production*, *testing*, dan *development*;
   - Pemilik perangkat TI dan informasi;
   - Spesifikasi perangkat keras dan lunak;
   - Dokumentasi proses bisnis;
   - Analisis dampak gangguan terhadap aset.
d) Apabila memungkinkan, identifikasi aset juga dapat dilakukan secara otomatis menggunakan *agent* yang dipasang dalam perangkat *host* atau jaringan.
e) Mengelompokkan aset berdasarkan klasifikasi dan tingkat kategori keamanan menurut aspek CIA.
f) Melakukan pembaruan secara berkala pada inventaris aset. Pembaruan ini bisa dilaksanakan tiap jangka waktu tertentu sesuai kebutuhan organisasi.

2. Identifikasi Kerentanan

Dalam pelaksanaan identifikasi kerentanan, TTIS dapat membagi proses tersebut menjadi tiga tahap yaitu tahap Pra Pelaksanaan, Pelaksanaan, dan Pasca Pelaksanaan. Tiap tahapan dilakukan agar proses identifikasi kerentanan berjalan secara efektif dan sistematis. Tahap Pra Pelaksanaan memiliki tujuan sebagai berikut:

a) Menentukan tim penguji dan waktu identifikasi kerentanan pada sistem elektronik. Tim penguji terdiri dari Ketua dan anggota tim penguji. Ketua tim bertugas untuk mengoordinasikan pelaksanaan identifikasi kerentanan dan anggota tim penguji.
b) Menentukan ruang lingkup identifikasi kerentanan pada sistem elektronik. Ruang lingkup sistem elektronik yang diuji merupakan kesepakatan antara pemilik sistem elektronik dan penguji.
c) Penandatanganan perjanjian kerahasiaan antara pemilik sistem elektronik dan tim penguji sebagai dasar hukum yang mengikat kedua belah pihak.
d) Menentukan jenis identifikasi kerentanan. Jika membutuhkan pengujian untuk keperluan identifikasi kerentanan harian, maka dapat menggunakan VA. Sedangkan PT dapat dipilih ketika menguji sistem baru, perubahan konfigurasi yang cukup banyak, atau dilakukan setahun sekali.
e) Menentukan kebutuhan dan metode identifikasi kerentanan pada sistem elektronik. Metode yang dapat dipilih adalah metode *black-box*, *gray-box*, atau *white-box*. Dari metode yang ditentukan, akan diidentifikasi kebutuhan *tools* dan informasi apa saja yang dibutuhkan.
f) Memastikan kesiapan pengujian. Sistem elektronik dipastikan sudah siap untuk dilakukan pengujian dengan memerhatikan risiko yang mungkin berdampak.

Pada Tahap Pelaksanaan, dilakukan serangkaian metodologi pengujian keamanan pada ruang lingkup yang telah ditentukan sebelumnya. Tahap pelaksanaan identifikasi kerentanan pada sistem elektronik dilaksanakan dengan memperhatikan hal-hal berikut:

a) Dilaksanakan *kick-off meeting* pada awal pelaksanaan sesuai dengan waktu yang telah disepakati. *Kick off meeting* menjadi penanda dimulainya proses identifikasi kerentanan pada sistem elektronik yang ditentukan.
b) Pencarian kerentanan dilaksanakan sesuai dengan metodologi dan ruang lingkup yang telah ditentukan. Penguji dapat menggunakan metodologi yang sudah ada seperti OWASP, OSSTMM, NIST, PTES, atau ISSAF.
c) Penguji melakukan eksploitasi pada kerentanan yang ditemukan. Kerentanan yang teridentifikasi maka harus dilakukan pembuktian (*Proof of Concept*).
d) Tim penguji melakukan dokumentasi pada kerentanan yang ditemukan.

Tahap terakhir pada proses identifikasi kerentanan adalah tahap pasca pelaksanaan. Pada tahap ini, dilakukan evaluasi hasil temuan serta penutupan proses pengujian. Tahap pasca pelaksanaan bertujuan untuk memastikan bahwa semua kerentanan yang ditemukan telah didokumentasikan dengan baik, solusi telah disiapkan, dan rekomendasi mitigasi diberikan kepada pemilik sistem. Berikut adalah langkah-langkah yang dapat dilakukan pada tahap pasca pelaksanaan:

a) Melakukan reviu dan penilaian kerentanan yang telah ditemukan dan pengklasifikasian kerentanan seperti kritis, tinggi, sedang, rendah, atau hanya sebatas informasi. Penilaian tingkat kerentanan dapat menggunakan alat seperti CVSS.
b) Menyiapkan laporan yang mencakup deskripsi kerentanan, dampak yang mungkin terjadi jika kerentanan tersebut tereksploitasi, serta rekomendasi remediasi kerentanan.
c) Memaparkan hasil temuan kerentanan dan memastikan bahwa kerentanan kritis tersampaikan kepada pemilik sistem elektronik untuk dilakukan tindakan remediasi secepatnya.
d) Menyerahkan laporan akhir temuan hasil pencarian kerentanan yang telah disahkan kepada pemilik sistem, disertai dengan saran

perbaikan dan rekomendasi jangka panjang untuk meningkatkan keamanan sistem.

Setelah seluruh tahapan ini dilalui, TTIS dapat menyusun strategi untuk meminimalkan risiko serupa di masa mendatang dengan memperbarui kebijakan keamanan dan melaksanakan pengujian berkala.

3. Laporan Kerentanan

TTIS perlu memiliki jalur komunikasi atau kontak yang dapat dihubungi oleh pihak eksternal dalam melaporkan kerentanan dari sistem yang dikelola. Jalur komunikasi laporan kerentanan dapat berupa *call center* atau dapat berbentuk penyelenggaran program Pengungkapan Kerentanan. Pada struktur TTIS, fungsi ini diampu oleh Unit Penanganan Kerentanan. Penjelasan tentang laporan kerentanan dapat merujuk pada subbagian tentang laporan kerentanan.

B. Tahap Prioritisasi

1. Validasi Kerentanan

Hasil pada tahap identifikasi diberikan pihak yang bertanggung jawab untuk memverifikasi/memvalidasi apakah kerentanan benar-benar ada dan dapat di eksploitasi. Verifikasi/validasi dapat dilakukan dengan mengikuti langkah-langkah yang ada pada proses identifikasi atau laporan kerentanan yang diterima. Terdapat beberapa hal yang perlu diperhatikan dalam melakukan proses verifikasi/validasi:

a) Perhatikan persyaratan dan detail lain yang dikirimkan pelapor untuk melakukan langkah-langkah dalam memproduksi kerentanan tersebut.
b) Jika tidak dapat memproduksi ulang kerentanan, hubungi pelapor (melalui tim tanggap insiden) untuk bekerja sama dan mengidentifikasi masalah lebih lanjut.

c) Jika kerentanan dianggap valid, organisasi harus mempertimbangkan hal-hal berikut:
   - Apakah kerentanan ada pada produk organisasi atau pada produk pihak ketiga?
   - Apakah ini duplikat dari kerentanan yang sudah pernah ditemukan?
   - Produk apa saja yang mungkin terdampak?
   - Apakah kerentanan sangat berdampak pada sistem?
   - Apakah ini masalah keamanan atau fungsional?

Laporan hasil verifikasi/validasi awal harus segera disampaikan ke tim tanggap insiden. Keputusan valid atau tidaknya kerentanan harus disampaikan dengan jelas dan tidak ambigu.

2. Penilaian Risiko

Langkah penilaian risiko dapat dilakukan dengan cara menentukan tingkat kritikalitas kerentanan yang ditemukan pada sistem. Pengukuran nilai risiko ini dapat dilakukan menggunakan standar CVSS terbaru dan NIST SP 800-30 dengan pertimbangan berdasarkan:

- Posisi aset (internal atau eksternal);
- Tingkat level prioritas aset;
- Jenis celah keamanan yang ditemukan;
- Peluang bagi penyerang untuk mendapatkan dan memanfaatkan celah tersebut;
- Dampak potensial kerentanan berdasarkan CIA;
- Dampak kerugian yang ditimbulkan dari risiko dengan skala deskriptif;
- Dokumentasi penilaian risiko sebelumnya.

Penilaian risiko menggunakan CVSS dilakukan dengan perhitungan berbasis formula untuk menetapkan skor keamanan pada kerentanan yang diidentifikasi. Untuk menggunakan CVSS, dapat mengakses CVSS *Calculator* secara online melalui peramban web. CVSS *Calculator* secara

mendasar dapat merujuk pada beberapa matriks yang digunakan untuk memberikan gambaran yang terstandardisasi dan terukur tentang Tingkat keparahan sebuah kerentanan. Terdapat beberapa matriks dalam penilaian dasar (*Base Metrics*). Berikut penjelasan setiap komponen pada *base metrics* CVSS:

***Exploitability Metrics*:**

Komponen yang digunakan untuk menilai seberapa mudah atau sulit sebuah kerentanan dapat dieksploitasi oleh penyerang.

a) *Attack Vektor* (AV)
   - Deskripsi: Digunakan untuk menunjukkan bagaimana penyerang dapat mengeksploitasi kerentanan yang ditemukan.
   - Nilai dan Penjelasan:
     a. *Network* (N): Kerentanan dapat dieksploitasi dari jarak jauh melalui jaringan internet.
     b. *Adjacent* (A): kerentanan dapat dieksploitasi dari jaringan yang sama dengan target secara fisik maupun logic (contoh : *Bluetooth*, NFC, IEEE 802.11, Local IP Subnet, VPN).
     c. *Local* (L): Kerentanan dapat dieksploitasi dengan cara melakukan akses langsung ke perangkat sistem (contoh: *keyboard, console*, ssh, *social engineering* untuk mengelabui pengguna yang sah membuka *file* berbahaya).
     d. *Physical:* kerentanan hanya dapat dieksploitasi dengan melakukan akses langsung ke fisik perangkat atau sistem target (contoh : *Evil Maid Attack*).

b) *Attack Complexity* (AC)
   - Deskripsi: digunakan untuk menggambarkan kompleksitas yang diperlukan dalam mengeksploitasi kerentanan.
   - Nilai dan Penjelasan:
     1) *Low* (L): Eksploitasi kerentanan dapat dilakukan dengan mudah tanpa memerlukan persyaratan khusus dan dapat dilakukan secara berulang.

2) *High* (H): Eksploitasi kerentanan memerlukan kondisi yang lebih khusus dan kompleks atau interaksi yang signifikan dari penyerang. Proses eksploitasi dapat dilakukan ketika serangkaian kondisi spesifik terpenuhi.

c) *Attack Requirements* (AT):
   - Deskripsi: komponen yang digunakan menggambarkan persyaratan tambahan yang diperlukan untuk melakukan eksploitasi kerentanan.
   - Nilai dan Penjelasan:
     1) *None* (N): tidak membutuhkan persyaratan tambahan yang diperlukan untuk mengeksploitasi kerentanan. Proses eksploitasi langsung dapat dilakukan setelah kerentanan ditemukan.
     2) *Present* (P): membutuhkan persyaratan tambahan yang diperlukan untuk mengeksploitasi kerentanan. Perlu adanya persyaratan atau pengetahuan khusus untuk eksploitasi setelah menemukan kerentanan.

d) *Privileges Required* (PR)
   - Deskripsi: Tingkat hak akses yang diperlukan penyerang untuk melakukan ekploitasi kerentanan.
   - Nilai dan Penjelasan:
     1) *None* (N): Penyerang tidak memerlukan hak akses apa pun untuk melakukan eksploitasi kerentanan.
     2) *Low* (L): Penyerang memerlukan hak akses terendah, seperti akun pengguna yang terbatas.
     3) *High* (H) : Penyerang memerlukan hak akses tertentu atau khusus seperti administrator.

e) *User Interaction* (UI)
   - Deskripsi: komponen yang digunakan untuk menunjukkan apakah interaksi pengguna diperlukan untuk mengeksploitasi kerentanan.
   - Nilai dan Penjelasan:

1) *None* (N): Eksploitasi kerentanan tidak memerlukan interaksi dari pengguna yang terpengaruh (Contoh: *Remote Code Execution*, *SQL Injection*).
2) *Required* (R): Penyerang memerlukan interaksi yang spesifik dari pengguna yang terpengaruh untuk mengeksploitasi kerentanan (contoh: *Phising*, *Social Engineering*, *Cross Site Scripting*).

Vulnerable System Impact Metrics

Komponen yang digunakan untuk menilai dampak dari eksploitasi kerentanan terhadap sistem yang rentan. Terdiri dari tiga sub-komponen utama sebagai berikut:

a) *Confidentiality* (VC):
- Deskripsi: Digunakan untuk mengukur potensi dampak kerahasiaan informasi jika kerentanan berhasil dieksploitasi.
- Nilai dan Penjelasan:
  1) None (N): Tidak berdampak pada kerahasiaan.
  2) Low (L): Eksploitasi kerentanan dapat mengungkapkan informasi yang terbatas (Contoh : Nama, email, foto profil, informasi profil umum).
  3) High (H): Eksploitasi kerentanan dapat mengungkapkan informasi yang sangat sensitif (contoh: password, kunci enkripsi, private key, data pribadi).

  Jika kerentanan mengizinkan penyerang untuk mengakses data pribadi pengguna, skor *Confidentiality* akan tinggi karena potensi pengungkapan informasi sensitif.

b) Integrity (VI):
- Deskripsi: Digunakan untuk mengukur potensi dampak integritas data jika kerentanan berhasil dieksploitasi.
- Nilai dan Penjelasan:
  1) None (N) : Tidak berdampak pada integritas data.

2) Low (L) : Eksploitasi kerentanan dapat menyebabkan modifikasi yang tidak signifikan pada data.
3) High (H): Eksploitasi kerentanan dapat mengungkapkan informasi yang sangat sensitif.

Jika kerentanan memungkinkan penyerang untuk memodifikasi atau menghapus data penting, skor *Integrity* akan tinggi karena potensi dampak pada integritas data.

c) Availability (VA):

- Deskripsi: Digunakan untuk mengukur potensi dampak ketersediaan sistem atau layanan jika kerentanan berhasil dieksploitasi.
- Nilai dan Penjelasan:
  1) None (N): Tidak berdampak pada ketersediaan sistem atau layanan.
  2) Low (L): Eksploitasi kerentanan dapat menyebabkan penurunan kinerja atau gangguan pada layanan yang tidak kritis atau penting.
  3) High (H) : Eksploitasi kerentanan dapat menyebabkan penurunan kinerja atau gangguan pada layanan yang kritis atau penting.

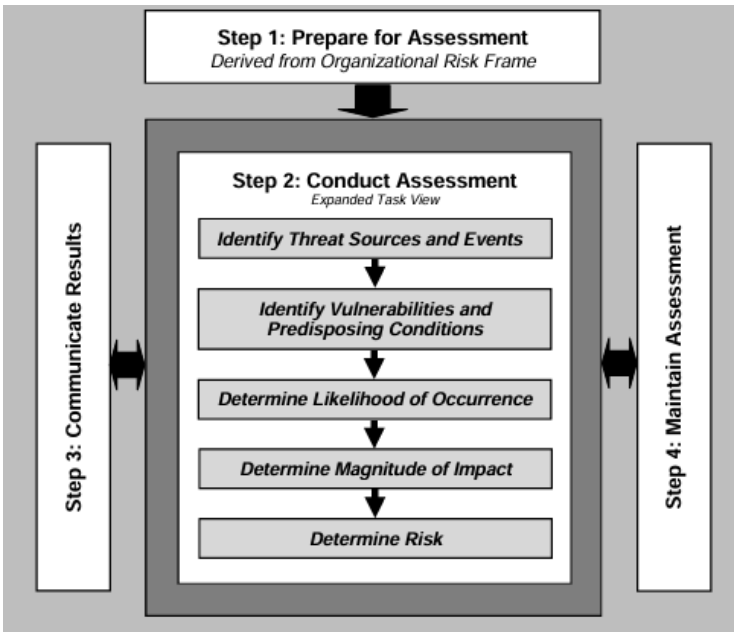
  Jika kerentanan menyebabkan sistem menjadi tidak dapat diakses oleh pengguna yang sah, skor *Availability* tinggi karena potensi dampak terhadap ketersediaan layanan.

Kerentanan yang teridentifikasi pada suatu sistem kemudian ditentukan nilai dari masing-masing metriknya. Nilai dari metrik-metrik tersebut dimasukkan ke dalam rumus CVSS 4.0 untuk menghasilkan skor seperti pada Tabel 4.

Tabel 4. Skor CVSS

Kategori	Skoring
None	0,0
Low	0,1 – 3,9
Medium	4,0 – 6,9
High	7,0 – 8,9
Critical	9,0 – 10,0

Penilaian risiko dengan menggunakan NIST SP 800-30 dapat mengikuti langkah-langkah dalam Gambar 19. Penjelasan tahapan penilaian risiko dapat dijelaskan sebagai berikut,



Gambar 19. Pelaksanaan Penilaian Risiko NIST SP 800-30

a) Tahap 1 : Mempersiapkan Penilaian Risiko

Pada tahap ini, ditentukan tujuan, ruang lingkup, toleransi risiko, sumber ancaman, kerentanan, dan dampak. Selain itu juga

ditentukan model risiko dan analisis yang digunakan dalam penilaian risiko.

b) Tahap 2 : Melaksanakan Penilaian Risiko

Pada tahap ini, dilakukan pencarian informasi terkait ancaman yang mungkin terjadi, potensi terjadinya ancaman, celah kerentanan yang dimanfaatkan, kemungkinan kerentanan tersebut dimanfaatkan, dampak yang ditimbulkan, dan nilai risiko berdasarkan informasi-informasi tersebut.

c) Tahap 3 : Membagikan Informasi Penilaian Risiko

Pada tahap ini, dilakukan penyampaian hasil penilaian risiko kepada pimpinan dan penyampaian informasi risiko yang relevan kepada anggota

d) Tahap 4 : Mengevaluasi Penilaian Risiko

Pada tahap ini, dilakukan monitoring berkelanjutan tentang faktor risiko dan melakukan pembaruan terhadap risiko yang ada.

3. Penentuan Prioritas

Setelah dilakukan identifikasi kerentanan, penting bagi TTIS untuk melakukan penilaian dan memperioritaskan kerentanan keamanan yang telah diidentifikasi dan tervalidasi kebenaranya. Penentuan prioritas penanganan kerentanan, dapat mempertimbangkan :

1. Apakah kerentanan berada pada sistem kritis (Critical System)?
2. Apa klasifikasi informasi yang terdapat pada sistem yang terkena dampak?
3. Apakah sistem yang terdampak digunakan oleh banyak pengguna publik?
4. Apakah sudah ada mitigasi yang dapat membatasi potensi dampak eksploitasi?
5. Dapatkah perangkat perimeter keamanan (IDS,IPS,EDR) berbasis jaringan atau host mendeteksi atau mencegah kerentanan?

6. Bisakah sistem dan prosedur organisasi efektif untuk merespon dan menangani dengan cepat terhadap masalah kerentanan atau eksploitasi yang terjadi?
7. Semakin tinggi nilai penilaian risiko, berbanding lurus dengan prioritas perbaikan.

Kerentanan yang dinilai sebagai risiko kritis bagi organisasi harus segera ditangani. Kerentanan kritis dapat ditentukan berdasarkan:

1. Kerentanan keamanan memungkinkan eksekusi kode jarak jauh.
2. Berdampak pada sistem penting organisasi.
3. Eksploitasi dapat dilakukan pada domain publik dan digunakan secara aktif.
4. Sistem terhubung ke internet dan tidak adanya proses mitigasi yang dilakukan.

C. Tahap Penanganan

1. Remediasi

Dalam melakukan proses remediasi TTIS harus melakukan analisis perhitungan tingkat kerentanan dan prioritisasi untuk menentukan jangka waktu remediasi yang direkomendasikan sebagaimana dijelaskan pada Tabel 5.

Tabel 5. Rekomendasi Jangka Waktu Remediasi

Tingkat Kerentanan	CVSS *Score*	Aset non-kritikal	Aset Kritikal
Low	< 4.0	Berdasarkan ketersediaan sumber daya	Berdasarkan ketersediaan sumber daya
Medium	4.0 – 6.9	< 9 bulan	< 6 bulan
High	7.0 – 8.9	< 3 bulan	< 1 bulan

Critical	9.0+	7 – 14 hari	1 - 3 hari

Untuk melakukan langkah remediasi pada kerentanan yang ditemukan, TTIS dapat merujuk tahapan remediasi berdasarkan ISO/IEC 30111:2019 yang terbagi ke dalam 3 tahapan:

1) Menentukan teknik remediasi yang akan dilakukan dengan mempertimbangkan waktu remediasi, tingkat risiko eksploitasi, dan langkah pengujian untuk memastikan teknik remediasi yang dilakukan tidak menimbulkan masalah baru
2) Menerapkan teknik remediasi yang telah ditentukan, yang dapat meliputi perbaikan kode sumber, pembaruan versi, dan/atau perubahan konfigurasi untuk menutup kerentanan yang teridentifikasi
3) Menguji hasil remediasi yang dilakukan untuk memastikan celah kerentanan dapat tertutup dan tidak menimbulkan kerentanan baru atau masalah lain yang mengganggu operasional sistem

Jika remediasi tidak dapat diselesaikan sesuai jangka waktu yang direkomendasikan atau celah kerentanan tidak dapat ditutup, maka TTIS harus melakukan langkah mitigasi terhadap kerentanan tersebut.

2. Mitigasi

Langkah mitigasi harus dilakukan oleh TTIS jika kerentanan tidak dapat diremediasi secara penuh oleh organisasi. Beberapa kondisi dan alasan yang dapat menjadi penyebab mitigasi harus dilakukan adalah jika langkah remediasi yang diperlukan dapat mengganggu berjalannya proses bisnis aplikasi, keterbatasan teknologi yang membutuhkan biaya, dan belum adanya *update/patch* yang disediakan oleh vendor teknologi terdampak. Untuk melakukan langkah mitigasi, TTIS disarankan untuk membuat rencana mitigasi kerentanan yang setidaknya meliputi namun tidak terbatas pada:

1) Penerapan kontrol keamanan untuk mitigasi kerentanan dalam bentuk penggunaan perangkat lunak/tools seperti *Security Information and Event Management* (SIEM), *Endpoint Detection*

and Response (EDR), *Next-Generation Firewalls* (NGFW), *Antivirus/Anti-Malware*, *Patch Management Systems*.

2) Penerapan *multi-factor authentication* (MFA) jika kerentanan bersumber dari adanya penggunaan mekanisme autentikasi yang kurang tepat atau kerentanan itu berasal dari fitur aplikasi yang berada pada sisi pengguna.
3) Pengisolasian sumber daya/perangkat yang rentan jika patching belum dapat dilakukan pada sumber daya/perangkat yang rentan.
4) Penghapusan atau penghentian penggunaan sumber daya/perangkat yang rentan jika tidak dapat diisolasi atau dilindung lagi
5) Peningkatan atau penggantian sumber daya/perangkat yang rentan ketika terdapat kerentanan yang tidak dapat diremediasi namun TTIS memiliki ketergantungan terhadap sumber daya/perangkat terkait

Sama halnya dengan remediasi, untuk menerapkan langkah mitigasi TTIS harus melakukan pengujian untuk memastikan bahwa langkah mitigasi yang dilakukan tidak menimbulkan kerentanan baru atau masalah lain yang mengganggu operasional sistem.

3. Penerimaan Risiko

Dalam hal remediasi dan mitigasi tidak dapat dilakukan dan risiko berada pada level yang diterima oleh TTIS, maka TTIS harus menerima risiko dan dampak yang mungkin terjadi dari adanya kerentanan tersebut. Dalam jangka waktu selama risiko tersebut diterima, TTIS harus senantiasa mencari informasi langkah remediasi yang dapat dilakukan terhadap kerentanan tersebut dan melakukan remediasi segera setelah cara penanganan kerentanan tersebut diketahui.

D. Tahap Verifikasi

1. Validasi Perbaikan

Tahapan validasi perbaikan bertujuan untuk memastikan bahwa remediasi atau perbaikan yang dilakukan efektif dalam mengatasi kerentanan tanpa menimbulkan masalah baru. Tahapan ini diampu oleh Unit Penanganan Kerentanan dan dapat berkoordinasi dengan pihak-pihak terkait, seperti pelapor kerentanan, tim uji penetrasi, dan juga pengembang sistem.

Tahapan validasi dapat dilakukan dengan beberapa tindakan berikut:

1) Pemindaian Kerentanan ulang, untuk memastikan kerentanan telah diperbaiki dengan baik;
2) Uji penetrasi terbatas pada area spesifik kerentanan yang telah diperbaiki/dimitigasi;
3) Berkolaborasi dengan pihak terkait, contohnya dalam hal kerentanan ditemukan oleh pihak eksternal, maka TTIS dapat meminta bantuan kepada pihak tersebut untuk menguji ulang kerentanan yang ditemukan;

Apabila dari hasil validasi ditemukan bahwa kerentanan belum diperbaiki/dimitigasi dengan baik, atau menimbulkan permasalahan baru, maka tahap penanganan kerentanan perlu diulang kembali.

2. Pelaporan

Hasil tindak lanjut penanganan kerentanan perlu didokumentasikan dengan baik, mencakup uraian langkah-langkah yang diambil dalam penanganan kerentanan. Dokumentasi dilaporkan kepada pemangku kepentingan terkait, termasuk pihak yang memberikan input kerentanan kepada TTIS. Sebagai contoh pada sebuah kerentanan yang dilaporkan oleh pihak eksternal melalui program pengungkapan kerentanan, maka TTIS perlu memberikan pelaporan tindakan yang telah diambil dalam menangani kerentanan kepada pelapor. Begitu pula apabila informasi kerentanan berasal dari sumber lainnya, seperti TTIS Nasional atau TTIS Sektoral, maka informasi tindakan penanganan

kerentanan perlu dilaporkan sebagai bentuk umpan balik atas kerentanan yang diinformasikan.

1) Dokumentasi pada Sistem Manajemen Kerentanan/ Repositori Kerentanan

TTIS dapat menyimpan semua dokumentasi laporan penanganan kerentanan pada suatu Sistem Manajemen Kerentanan atau repositori kerentanan, sehingga informasi dapat tersimpan dengan baik dan dapat menjadi referensi di masa mendatang serta dapat dijadikan pembelajaran dalam pengembangan sistem dan kebijakan keamanan.

2) Berbagi Informasi

Kolaborasi lebih lanjut dapat dilakukan dengan berbagi informasi kerentanan serta penanganan yang efektif dengan sesama TTIS organisasi lain, dalam satu sektor yang sama atau secara nasional. Tugas dan fungsi ini dapat diampu oleh Unit Pembinaan dan Publikasi pada TTIS organisasi yang dikoordinasikan oleh TTIS Nasional maupun TTIS Sektoral.

E. Tahap Evaluasi

Dalam pelaksanaan evaluasi manajemen kerentanan pada organisasi, tim tanggap insiden siber dapat menggunakan beberapa metrik penilaian. Metrik yang digunakan untuk penilaian berfokus pada efektivitas remediasi pada sistem (Office of the CISO, 2024). Dengan mengetahui tingkat efektivitas dan efisiensi dari pengelolaan kerentanan yang telah dilakukan, maka pemangku kepentingan dapat menentukan arah kebijakan yang akan diambil. Metrik penilaian yang digunakan untuk melakukan evaluasi proses manajemen kerentanan dapat berupa pertanyaan-pertanyaan seperti berikut:

1) Apakah proses identifikasi kerentanan sudah terselenggara secara efektif?
2) Apakah aset-aset yang teridentifikasi rentan sudah diprioritaskan dengan benar?

3) Seberapa besar nilai kerugian jika kerentanan suatu aset tereksploitasi?
4) Bagaimana pemangku kepentingan merespons kerentanan yang teridentifikasi?
5) Apakah ada hal-hal yang menghambat proses remediasi kerentanan?
6) Seberapa cepat proses remediasi pada kerentanan yang teridentifikasi?
7) Apa parameter risiko suatu kerentanan bisa diterima?
8) Apakah proses validasi hasil remediasi kerentanan sudah dilakukan dengan benar?
9) Apakah proses manajemen kerentanan sudah diterapkan sesuai *Service Level Agreement*?

Jawaban dari metrik penilaian yang telah ditentukan dapat digunakan organisasi sebagai pembelajaran yang dapat dipetik dari proses manajemen kerentanan yang telah dilakukan. Selain evaluasi berdasarkan langkah-langkah dalam pengelolaan kerentanan, evaluasi juga dapat berupa pengembangan VM dengan cara menyelenggarakan pelatihan bagi personil penyelenggara manajemen kerentanan, penyusunan kebijakan penyelenggaraan, serta koordinasi dan kolaborasi secara berkelanjutan bagi pihak-pihak terkait. Dengan begitu, proses penyelenggaraan manajemen kerentanan dapat terus berkembang dan bisa menyesuaikan dengan tren keamanan siber di Indonesia.

BAB VII
PENGEMBANGAN BAKAT TERKAIT MANAJEMEN KERENTANAN

In the interconnected world, your cybersecurity is only as strong as the weakest link in your supply chain

- Anonymus

A. Peta Okupasi

Peta okupasi adalah dokumen yang menyediakan informasi tentang pemetaan jabatan, okupasi, atau profesi dalam berbagai bidang, sub bidang, dan area fungsi di semua jenis pekerjaan, seperti dijelaskan oleh Bappenas (2024). Pada tahun 2019, BSSN, yang merupakan lembaga yang berfokus pada keamanan siber, telah menerbitkan peta okupasi khusus untuk area fungsi keamanan siber (BSSN, 2019). Dokumen ini mendetailkan 30 okupasi dalam keamanan siber yang berada pada level 5-9. Okupasi dalam keamanan siber termasuk ke dalam kelompok jabatan teknisi atau analis (level 4-6) dan kelompok jabatan ahli (level 7-9). Dari total 30 okupasi yang tercantum, lima di antaranya secara spesifik berhubungan dengan manajemen kerentanan, sebagaimana dijelaskan dalam Tabel 6 (BSSN, 2019).

Tabel 6. Peta okupasi dalam kerangka kualifikasi nasional Indonesia pada area fungsi keamanan siber

Kode	Nama Okupasi	Deskripsi	Profil	Syarat	Tugas Utama
100508.06	Cybersecurity Operator	Kemampuan dan keterampilan untuk mengategorikan dan mengenali tingkat kerawanan suatu insiden keamanan siber, bertugas untuk melaksanakan prosedur-prosedur dan perintah dari pejabat di atasnya pada pusat operasi keamanan/Security Operation Center.	1. Berintegritas 2. Mematuhi prosedur 3. Berorientasi pada detail 4. Komunikatif 5. Mampu bekerja dalam tim	KKNI Level 4	1. Mendeteksi kerentanan 2. Mengumpulkan data yang diperlukan untuk memenuhi persyaratan pelaporan insiden keamanan siber 3. Mematuhi prosedur terminasi sistem dan tata cara pelaporan insiden

Kode	Nama Okupasi	Deskripsi	Profil	Syarat	Tugas Utama
100601.03	Cyber Security Analyst/ Cybersecurity Incident Analyst	Kemampuan dan keterampilan untuk menindaklanjuti tiket insiden, menganalisis insiden, memantau penanganan insiden dan ancaman keamanan dalam suatu organisasi, serta bertugas untuk melaksanakan prosedur-prosedur dan perintah dari pejabat di atasnya pada pusat operasi keamanan/ Security Operation Center.	1. Berintegritas 2. Mematuhi prosedur 3. Berorientasi pada detail 4. Komunikatif 5. Mampu bekerja dalam tim	1. KKNI Level 5 2. Memiliki pengalaman sebagai tim CSIRT 3. Memiliki Sertifikasi okupasi Cybersecurity Operator	1. Koordinasi penanganan insiden dan manajemen krisis 2. Mendeteksi Kerentanan 3. Memberikan arahan mengenai solusi masalah keamanan siber yang teridentifikasi 4. Berkoordinasi dengan penegakan hukum selama insiden keamanan 5. Menyusun laporan insiden rinci dan ringkasan teknis untuk manajemen, administrator dan *end-user liaison* dengan entitas analisis ancaman cyber lainnya

Kode	Nama Okupasi	Deskripsi	Profil	Syarat	Tugas Utama
100606.04	Vulnerability Assessment Analyst	Kemampuan dan keahlian untuk melakukan *assessment* terhadap celah keamanan dalam sebuah sistem pada sebuah organisasi	1. Berintegritas 2. Analitis 3. Berorientasi pada detail 4. Mampu bekerja dalam tim	1. Memiliki KKNI Level 5 2. Memiliki pengetahuan terkait keamanan siber, ancaman keamanan siber dan metode assessment	1. Melakukan reconnaissance (pengumpulan informasi) mengenai target baik aktif maupun pasif 2. Melakukan scanning 3. Melakukan enumeration 4. Melakukan vulnerability assessment 5. Menyusun laporan dan mengkomunikasikan hasil laporan

Kode	Nama Okupasi	Deskripsi	Profil	Syarat	Tugas Utama
100725.06	Threat Hunter	Kemampuan teknis dan keahlian untuk melakukan identifikasi ancaman tersembunyi yang mungkin telah masuk tanpa terdeteksi di dalam sistem serta bertugas untuk melaksanakan prosedur-prosedur dan perintah dari pejabat di atasnya pada pusat operasi keamanan/Security Operation Center.	1. Berintegritas 2. Mengatasi masalah (problem solving) 3. Analitis 4. Berorientasi pada detail 5. Bekerja dalam tim	1. KKNI Level 6 2. Lulusan S1 3. Memiliki pengalaman sekurang-kurangnya 2 tahun sebagai tim CSIRT 4. Memiliki Sertifikasi okupasi Penetration Tester, atau Vulnerability Assessment Analyst atau Cybersecurity Analyst/Cybersecurity Incident Analyst	1. Melakukan pemantauan terhadap aktivitas yang rentan ancaman 2. Mengidentifikasi serangan-serangan terhadap kontrol akses 3. Mendeteksi kerentanan keamanan dan potensi pelanggaran 4. Menyusun laporan dan mengkomunikasikan hasil laporan

Kode	Nama Okupasi	Deskripsi	Profil	Syarat	Tugas Utama
100726.04	Penetration Tester	Kemampuan teknis dan keahlian untuk menguji atau mengevaluasi keamanan sistem elektronik dengan berusaha mengambil alih sistem tersebut dengan menggunakan teknik atau tool yang sama dengan digunakan oleh penyerang	1. Berintegritas 2. Sintesis 3. Independen 4. Objektif 5. Kritis 6. Berorientasi pada hasil	1. KKNI Level 6 2. Memiliki dasar pengetahuan tentang cara bekerja sistem komputer dan aplikasinya 3. Memiliki Sertifikasi okupasi Vulnerability Assessment Analyst	1. Melakukan *reconnaissance* (pengumpulan informasi) mengenai target baik aktif maupun pasif 2. Melakukan *scanning* 3. Melakukan enumeration 4. Melakukan vulnerability assessment 5. Melakukan eksploitasi Menyusun laporan dan mengkomunikasikan hasil laporan

B. Kursus/sertifikasi Terkait

1. Level Nasional

Berdasarkan Keputusan Kepala BNSP Nomor Kep 1142/BNSP/V/2024, Lembaga Sertifikasi Profesi BSSN menyelenggarakan berbagai skema sertifikasi okupasi di bidang keamanan siber. Skema yang terkait dengan manajemen kerentanan diuraikan dalam Tabel 7.

Tabel 7. Skema sertifikasi LSP BSSN yang terkait dengan Manajemen Kerentanan

No	Skema Sertifikasi	Unit Kompetensi	
		Kode Unit	Judul Unit Kompetensi
1	L1 SOC-Analyst	J.62SOC00.005.1	Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali
		J.62SOC00.006.1	Melakukan Deteksi Kerentanan Aset Teknologi Informasi (TI)
		J.62SOC00.008.1	Melakukan Pemantauan Aset Teknologi Informasi (TI) terhadap Aktivitas Ancaman Siber
		J.62SOC00.010.1	Memberikan Tiket terhadap Insiden Keamanan Siber
		J.62SOC00.011.1	Menganalisis *Log* pada Security Operations Center (SOC)
		J.62SOC00.018.1	Menganalisis Dampak Insiden Keamanan Siber
2	Junior Penetration Tester	J.62UKS00.005.1	Mengumpulkan Informasi yang diperlukan untuk Pengujian Keamanan Siber
		J.62UKS00.006.1	Mencari Kerentanan Sesuai Ruang Lingkup Pengujian Keamanan Siber
		J.62UKS00.007.1	Menguji Kerentanan pada Objek Pengujian

No	Skema Sertifikasi	Unit Kompetensi	
		Kode Unit	Judul Unit Kompetensi
		J.62UKS00.009.1	Melakukan Kompilasi Temuan Hasil Pengujian Keamanan Siber
		J.62UKS00.010.1	Menyusun Laporan Hasil Pengujian Keamanan Siber
3	L2 SOC-Analyst	J.62S0C00.005.1	Melakukan Analisis Keamanan Siber terhadap Insiden Keamanan Siber untuk Menentukan Kendali
		J.62SOC00.006.1	Melakukan Deteksi Kerentanan Aset Teknologi Informasi (TI)
		J.62SOC00.007.1	Menganalisis Ancaman/ Anomali Keamanan Siber (*Threat intelligence*) pada Perimeter Keamanan
		J.62SOC00.008.1	Melakukan Pemantauan Aset Teknologi Informasi (TI) terhadap Aktivitas Ancaman Siber
		J.62SOC00.011.1	Menganalisis Log pada Security Operations Center (SOC)
		J.62SOC00.012.1	Melakukan Pencadangan Data Security Operations Center (SOC)
		J.62SOC00.018.1	Menganalisis Dampak Insiden Keamanan Siber
4	L3 SOC-Analyst	J.62SOC00.003.1	Menyusun Prosedur Penanganan Insiden Keamanan Siber
		J.62SOC00.007.1	Menganalisis Ancaman/Anomali Keamanan Siber (*Threat intelligence*) pada Perimeter Keamanan
		J.62SOC00.008.1	Melakukan Pemantauan Aset Teknologi Informasi (TI) terhadap Aktivitas Ancaman Siber
		J.62SOC00.014.1	Melakukan Investigasi Modus Operandi Insiden Keamanan Siber
		J.62SOC00.015.1	Mengidentifikasi Solusi Teknis terhadap Insiden Keamanan Siber yang Terjadi

No	Skema Sertifikasi	Unit Kompetensi	
		Kode Unit	Judul Unit Kompetensi
		J.62SOC00.016.1	Mengisolasi Aset Teknologi Informasi (TI) yangTerdampak untuk Menghentikan\ Insiden Keamanan Siber
		J.62SOC00.017.1	Melakukan Terminasi Layanan Aset Teknologi Informasi Terdampak (TI) Insiden untuk Perbaikan
		J.62SOC00.018.1	Menganalisis Dampak Insiden Keamanan Siber
		J.62SOC00.020.1	Membuat Rekomendasi Perbaikan setelah Insiden Keamanan Siber
5	Penetration Tester	J.62UKS00.001.1	Merencanakan Prosedur Uji Keamanan Siber
		J.62UKS00.002.1	Menentukan Metode Penilaian Kerentanan
		J.62UKS00.005.1	Mengumpulkan Informasi yang diperlukan untuk Pengujian Keamanan Siber
		J.62UKS00.006.1	Mencari Kerentanan sesuai Ruang Lingkup Pengujian Keamanan Siber
		J.62UKS00.007.1	Menguji Kerentanan pada Objek Pengujian
		J.62UKS00.008.1	Melakukan Kegiatan setelah Eksploitasi berdasarkan Ruang Lingkup Pengujian Keamanan Siber
		J.62UKS00.009.1	Melakukan Kompilasi Temuan Hasil Pengujian Keamanan Siber
		J.62UKS00.010.1	Menyusun Laporan Hasil Pengujian Keamanan Siber
6	Senior Penetration Tester	J.62UKS00.001.1	Merencanakan Prosedur Uji Keamanan Siber
		J.62UKS00.002.1	Menentukan Metode Penilaian Kerentanan
		J.62UKS00.003.1	Menentukan Ruang Lingkup Pengujian Keamanan Siber

No	Skema Sertifikasi	Unit Kompetensi	
		Kode Unit	Judul Unit Kompetensi
		J.62UKS00.004.1	Menentukan Tim Penguji Keamanan Siber
		J.62UKS00.005.1	Mengumpulkan Informasi yang diperlukan untuk Pengujian Keamanan Siber
		J.62K500.006.1	Mencari Kerentanan Sesuai Ruang Lingkup Pengujian Keamanan Siber
		J.62UKS00.007.1	Menguji Kerentanan pada Objek Pengujian
		J.62UKS00.008.1	Melakukan kegiatan setelah Eksploitasi berdasarkan Ruang Lingkup Pengujian Keamanan Siber
		J.62UKS00.009.1	Melakukan Kompilasi Temuan Hasil Pengujian Keamanan Siber
		J.62UKS00.010.1	Menyusun Laporan Hasil Pengujian Keamanan Siber
7	Incident Response Analyst	J.62SOC00.012.1	Melakukan Pencadangan Data Security Operations Center (SOC)
		J.62SOC00.013.1	Mengkomunikasikan Penanganan Insiden Keamanan Siber dan Manajemen Krisis
		J.62SOC00.014.1	Melakukan investigasi Modus Operandi Insiden Keamanan Siber
		J.62SOC00.015.1	Mengidentifikasi Solusi Teknis terhadap Insiden Keamanan Siber yang Terjadi
		J.62SOC00.016.1	Mengisolasi Aset Teknologi Informasi (TI) yang Terdampak untuk Menghentikan Insiden Keamanan Siber
		J.62SOC00.017.1	Melakukan Terminasi Layanan Aset Teknologi Informasi (TI) Terdampak Insiden untuk Perbaikan
		J.62SOC00.018.1	Menganalisis Dampak Insiden Keamanan Siber

No	Skema Sertifikasi	Unit Kompetensi	
		Kode Unit	Judul Unit Kompetensi
		J.62SOC00.020.1	Membuat Rekomendasi Perbaikan setelah Insiden Keamanan Siber

2. Level Internasional

Penyelenggara sertifikasi yang terkait dengan manajemen kerentanan mencakup berbagai organisasi terkemuka di bidang keamanan siber. *Offensive Security* dikenal dengan pendekatan praktis dalam uji penetrasi dan eksploitasi kerentanan, sementara EC-Council menawarkan beragam sertifikasi seperti CEH, CPENT, dan CTIA yang fokus pada keamanan jaringan, intelijen ancaman, dan penanganan insiden. (ISC)² menyediakan sertifikasi CISSP dan CCSP, yang menekankan pada keamanan informasi dan *cloud*. CompTIA menawarkan Security+, sebuah sertifikasi entry-level yang mencakup dasar-dasar keamanan. GIAC (*Global Information Assurance Certification*) berfokus pada evaluasi kerentanan perusahaan dan penggunaan alat keamanan tingkat lanjut, sementara CREST menyediakan sertifikasi uji penetrasi untuk aplikasi dan infrastruktur. Mile2 menawarkan CVA dan CEVA untuk penilaian kerentanan, dan ISACA menyediakan CISA serta CISM, yang mencakup audit dan manajemen keamanan informasi. PECB mendukung sertifikasi ISO terkait manajemen risiko, menambahkan dimensi tata kelola dan kepatuhan. Tabel 8 menyajikan sertifikasi internasional yang terkait langsung dengan manajemen kerentanan.

Tabel 8. Sertifikasi Internasional terkait dengan Manajemen Kerentanan

No.	Nama Sertifikasi	Deskripsi	Vendor/Penyedia
1	*Offensive Security Certified Professional (OSCP)*	Sertifikasi yang menguji kemampuan melakukan uji penetrasi dalam lingkungan yang terkendali, fokus pada penggunaan metode dan eksploitasi manual.	Offensive Security

No.	Nama Sertifikasi	Deskripsi	Vendor/Penyedia
2	*Certified Penetration Testing Professional (CPENT)*	Sertifikasi yang menilai keterampilan uji penetrasi lanjutan dalam lingkungan peretasan dunia nyata, termasuk jaringan yang rumit dan target hybrid.	EC-Council
3	*Certified Information Systems Security Professional (CISSP)*	Sertifikasi keamanan informasi untuk profesional yang berpengalaman dalam desain, pengelolaan, dan pemeliharaan arsitektur keamanan informasi.	(ISC)²
4	*EC-Council Certified Incident Handler (ECIH)*	Sertifikasi yang fokus pada pengelolaan insiden keamanan siber, dengan keterampilan mengidentifikasi, menanggapi, dan memitigasi serangan siber.	EC-Council
5	*Certified Ethical Hacker (CEH)*	Sertifikasi yang mengajarkan metode peretasan etis untuk mengidentifikasi kerentanan keamanan dalam sistem, termasuk teknik uji penetrasi.	EC-Council
6	*CompTIA Security+*	Sertifikasi entry-level yang menilai dasar-dasar keamanan siber, seperti manajemen risiko, kriptografi, dan keamanan jaringan.	CompTIA
7	*Certified Threat intelligence Analyst (CTIA)*	Sertifikasi yang membekali profesional dengan keterampilan untuk menganalisis, menafsirkan, dan merespons ancaman berbasis intelijen.	EC-Council

No.	Nama Sertifikasi	Deskripsi	Vendor/Penyedia
8	*GIAC Certified Vulnerability Assessor (GCVA)*	Sertifikasi yang mengukur keterampilan dalam mengidentifikasi dan menilai kerentanan dalam sistem dan jaringan, menggunakan berbagai alat keamanan.	GIAC
9	*CREST Certified Tester - Application (CCT APP)*	Sertifikasi yang memvalidasi keahlian dalam uji penetrasi aplikasi, termasuk aplikasi web, *mobile*, dan infrastruktur yang mendukungnya.	CREST
10	*CREST Certified Tester - Infrastructure (CCT INF)*	Sertifikasi yang menguji keterampilan melakukan uji penetrasi pada infrastruktur TI, termasuk jaringan dan sistem operasi.	CREST
11	*Certified Vulnerability Assessor (CVA)*	Sertifikasi yang berfokus pada kemampuan untuk mengidentifikasi, menganalisis, dan mengelola kerentanan dalam infrastruktur jaringan dan aplikasi.	Mile2
12	*Certified Expert Vulnerability Assessor (CEVA)*	Sertifikasi lanjutan yang mendalami keterampilan dalam mengelola dan memitigasi kerentanan, serta menilai risiko keamanan dengan lebih mendalam.	Mile2
13	*Certified Information Systems Auditor (CISA)*	Sertifikasi yang mencakup manajemen keamanan informasi, termasuk audit, pengendalian, dan pemantauan sistem IT untuk mendeteksi dan memperbaiki kerentanan.	ISACA

No.	Nama Sertifikasi	Deskripsi	Vendor/Penyedia
14	*GIAC Certified Enterprise Vulnerability Assessor (GEVA)*	Sertifikasi yang menguji keterampilan dalam mengelola kerentanan di lingkungan perusahaan besar, dengan fokus pada penilaian sistem yang kompleks dan beragam.	GIAC
15	*Offensive Security Web Expert (OSWE)*	Sertifikasi yang menguji kemampuan untuk menemukan dan mengeksploitasi kerentanan pada aplikasi web, dengan pendekatan manual.	Offensive Security
16	*ISO/IEC 27005 Risk Manager*	Sertifikasi yang fokus pada manajemen risiko keamanan informasi, termasuk identifikasi dan mitigasi kerentanan sebagai bagian dari proses manajemen risiko.	PECB
17	*Certified Information Security Manager (CISM)*	Sertifikasi yang berfokus pada pengelolaan program keamanan informasi, termasuk mitigasi kerentanan dan pengelolaan risiko.	ISACA
18	*Certified Cloud Security Professional (CCSP)*	Sertifikasi yang mencakup keamanan di lingkungan cloud, termasuk identifikasi dan mitigasi kerentanan cloud computing.	(ISC)²

Berdasarkan Standar Kompetensi Nasional dan Sertifikasi Level Internasional, terdapat pembagian kebutuhan kompetensi yang disesuaikan dengan langkah-langkah manajemen kerentanan. Tabel 9 menunjukkan beberapa contoh pembagian kompetensi sesuai dengan tahapan dalam manajemen kerentanan yang dibuat

Tabel 9. Pembagian kompetensi pada tiap tahapan

No	Langkah Manajemen Kerentanan	Sertifikasi Terkait	
		Standar Kompetensi Nasional	Standar Sertifikasi Level Internasional
1	Tahap Identifikasi	– L1 SOC-Analyst – Asisten Auditor Keamanan Informasi – Junior Penetration Tester – Incident Response Analyst	– CEH – OSCP – CPENT – ECIH – CompTIA Security+ – CTIA – GCVA – CCT APP – CCT INF – CEVA – GEVA – OSWE – CCSP – ISO 27001 Lead Implementer
2	Tahap Prioritisasi	– Asisten Auditor Keamanan Informasi/Auditor Keamanan Informasi – L2 SOC-Analyst/L3 SOC-Analyst	– CISSP – CISA – ISO/IEC 27005 Risk Manager – ISO 27001 Lead Implementer – ISO 27001 Lead Auditor – CompTIA Security+ – CVA – CISM
3	Tahap Penanganan	– Incident Response Analyst – L2 SOC-Analyst/L3 SOC-Analyst – Junior Penetration Tester – Penetration Tester/Senior Penetration Tester – Asisten Auditor Keamanan	– CEH – OSCP – CPENT – ECIH – CompTIA Security+ – CTIA – GCVA – CCT APP – CCT INF – CEVA – GEVA

No	Langkah Manajemen Kerentanan	Sertifikasi Terkait	
		Standar Kompetensi Nasional	**Standar Sertifikasi Level Internasional**
		Informasi/Auditor Keamanan Informasi	– OSWE – CCSP – ISO 27001 Lead Implementer – CISA – ISO/IEC 27005 Risk Manager – ISO 27001 Lead Implementer – ISO 27001 Lead Auditor – CVA – CISM – CISSP
5	Tahap Verifikasi	– L1 SOC-Analyst – Asisten Auditor Keamanan Informasi – Junior Penetration Tester – Incident Response Analyst	– CEH – CPENT – CompTIA Security+ – GCVA – CCT APP – CCT INF – CEVA – GEVA – OSWE – CCSP – ISO 27001 Lead Implementer – CVA – CISM
6	Tahap Evaluasi	– L3 SOC-Analyst – Auditor Keamanan Informasi – Senior Penetration Tester	– OSCP – ISO 27001 Lead Auditor – CPENT – CISSP – CEVA – CISA

C. Kode Etik Pegiat Keamanan Siber

Menurut Matwyshyn et al. (2010), norma-norma dalam penelitian kerentanan:

1) Membuat publikasi yang jelas terkait obyek manajemen kerentanan

   Obyek manajemen kerentanan ditujukan pada aset TI milik organisasi. Dalam rangka penyelenggaraan manajemen kerentanan, informasi terkait hal tersebut harus melalui publikasi yang resmi dan memuat cakupan obyek manajemen kerentanan dengan jelas sehingga pelaksanaannya dapat dilakukan dengan tepat. Publikasi ini dapat dilakukan melalui web resmi organisasi tentang detail obyek manajemen kerentanan dan dapat diakses secara umum.

2) Memahami Landasan Hukum yang Digunakan

   Sebelum melakukan rangkaian manajemen kerentanan, diperlukan adanya pemahaman terhadap peraturan atau legalitas oleh masing-masing pihak di dalamnya. Landasan hukum ini dapat diketahui dengan melakukan konsultasi terhadap firma-firma hukum atau instansi tertentu yang menaungi keamanan informasi dan kepentingan publik.

3) Menerapkan perlindungan data dengan baik

   Data sensitif seperti informasi pribadi, keuangan, dan informasi lain yang merujuk pada suatu pihak merupakan data yang harus dilindungi. Pihak-pihak yang terlibat dalam rangkaian manajemen kerentanan harus menerapkan beberapa langkah perlindungan sebagai berikut,

   a) Menggunakan praktik terbaik perlindungan data sensitif

      Setiap pihak dalam rangkaian manajemen kerentanan harus menerapkan kebijakan yang bertujuan untuk melindungi data. Seperti contoh, informasi terbatas hanya dapat diketahui oleh

internal tim dan tidak boleh dibagikan terhadap pihak di luar tim tersebut.

b) Membatasi akses terhadap data sensitif
   Data sensitif harus dilakukan penerapan pembatasan akses terhadap orang-orang yang tidak berhak mengetahuinya.

c) Membuat anonim data
   Data-data yang bersifat sensitif dapat disamarkan dengan cara menghapus detail tentang informasi yang merujuk terhadap suatu entitas. Selain itu, juga dapat dilakukan dengan menggantinya ke dalam kode atau penyebutan tertentu.

d) Melakukan berbagi informasi penelitian kerentanan
   Informasi tentang penelitian kerentanan baik berupa temuan kerentanan hingga remediasi kerentanan dapat dibagikan secara luas sebagai khazanah ilmu pengetahuan dengan mempertimbangkan keamanan data sensitif. Hal ini bermanfaat untuk meningkatkan kompetensi dan kolaborasi antar pihak dalam manajemen kerentanan.

e) Memahami alur untuk melaporkan kerentanan
   Dalam memberikan laporan kerentanan, laporan tersebut harus dilaporkan kepada orang yang tepat. Laporan tersebut juga harus dikirimkan melalui saluran yang tepat dan disediakan oleh pemilik aset TI.

f) Melakukan regenerasi dan pembelajaran berkelanjutan
   Rangkaian manajemen kerentanan merupakan suatu proses berkelanjutan yang mengikuti perkembangan teknologi dan arus informasi. Oleh karena itu, proses regenerasi pihak-pihak di dalamnya dan berbagi pengetahuan harus dilakukan untuk menunjang peningkatan dan pelaksanaan manajemen kerentanan.

BAB VIII
POIN DETERMINASI DAN SOLUSI

Kedaulatan siber adalah hal yang tidak bisa ditawar-tawar. Untuk mencapainya, kita harus membangun sumber daya manusia yang kompeten di bidang keamanan siber

- Hinsa Siburian, Kepala Badan Siber dan Sandi Negara

A. POIN DETERMINASI

1) Manajemen kerentanan sangat penting dalam memastikan sistem informasi tetap terlindungi dari ancaman yang terus berkembang. Dengan pemantauan secara rutin, organisasi dapat mendeteksi anomali trafik, aktivitas *malware*, dan potensi serangan lainnya yang dapat mengganggu operasional. Pemantauan yang terus-menerus menjadi langkah vital untuk menjaga keamanan sistem di tengah semakin meningkatnya risiko siber.
2) Setiap pemangku kepentingan dalam ekosistem keamanan siber, seperti peneliti, vendor, pengguna akhir, dan regulator, memiliki peran yang berbeda dalam mengidentifikasi, mengatasi, dan mengelola kerentanan. Kolaborasi antar pemangku kepentingan sangat penting untuk memastikan pengelolaan kerentanan yang efektif dan mengurangi risiko serangan yang dapat merugikan berbagai pihak.
3) Setelah kerentanan diidentifikasi, langkah remediasi atau mitigasi harus diambil berdasarkan tingkat prioritas dan dampak potensial yang ditimbulkan. Proses mitigasi yang terstruktur ini memastikan bahwa ancaman dengan risiko tertinggi menjadi fokus utama sehingga perlindungan terhadap sistem dapat dioptimalkan.
4) Di Indonesia, pengelolaan kerentanan didukung oleh kerangka regulasi yang kuat, seperti UU ITE, PP No. 71 Tahun 2019, serta berbagai peraturan dari BSSN. Regulasi-regulasi ini menyediakan landasan hukum yang jelas bagi organisasi dalam memperkuat keamanan siber dan memastikan kepatuhan terhadap standar keamanan yang berlaku.
5) Manajemen kerentanan bukan hanya sekadar respons terhadap ancaman, tetapi harus menjadi proses yang berkelanjutan. Langkah proaktif seperti *vulnerability assessment*, *penetration testing*, serta pembaruan sistem secara berkala merupakan bagian penting dari

strategi untuk menjaga ketahanan sistem terhadap serangan siber yang terus berkembang.

B. SOLUSI

1) Sistem deteksi dini dan tanggapan terhadap serangan siber perlu ditingkatkan melalui implementasi alat *threat intelligence* yang canggih serta pemantauan jaringan secara waktu nyata. Peningkatan ini akan mempercepat respons terhadap ancaman dan meningkatkan peluang mitigasi sebelum serangan meluas.
2) Kolaborasi antara pemerintah, sektor swasta, dan penyedia layanan keamanan harus diperkuat untuk berbagi informasi terkait kerentanan dan solusi mitigasi. Hal ini dapat diwujudkan melalui forum nasional dan internasional yang lebih efektif.
3) Keterlibatan masyarakat dalam melaporkan kerentanan perlu ditingkatkan melalui program pengungkapan yang terstruktur, serta memperkuat kampanye edukasi bagi masyarakat umum dan perusahaan tentang pentingnya keamanan data dan manajemen risiko.
4) Infrastruktur yang rentan, terutama yang masih menggunakan protokol usang seperti SMBv1, harus segera diperbarui dan diamankan. Pembaruan sistem dan *patch* secara berkala perlu diterapkan untuk memastikan perangkat lunak dan perangkat keras selalu dalam kondisi aman.
5) Setiap institusi, baik di sektor publik maupun swasta, harus memperkuat kemampuan tim tanggap insiden (CSIRT) untuk secara proaktif menangani ancaman siber. Tim ini harus diberikan pelatihan khusus dalam deteksi, pemulihan, dan mitigasi serangan.

DAFTAR PUSTAKA

AusCERT. (2024). *AusCERT RFC 2350: Description of AusCERT's Incident Response Service*. https://auscert.org.au/publications/policies-and-agreements/auscert-rfc2350/

Bappenas. (2024). *Peta Okupasi Nasional*. https://petaokupasi.bappenas.go.id/

Booth, H., Rike, D., & Witte, G. (2013). The National Vulnerability Database (NVD): Overview. *ITL Bulletin*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=915172

BSSN. (2019). *Peta Okupasi Nasional Keamanan Siber*. https://www.bssn.go.id

BSSN. (2021). *COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) STARTER KIT v1.0*.

BSSN. (2024). *Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber*.

Bugcrowd. (2022). *Reporting a Bug*. https://docs.bugcrowd.com/researchers/reporting-managing-submissions/reporting-a-bug/

CERT-Bund. (2024). *RFC 2350: CERT-Bund Description according to RFC 2350*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KRITIS/rfc2350_CERT-Bund_txt.html

CERT-EU. (2024). *RFC2350: CERT-EU Description according to RFC 2350*. https://www.cert.europa.eu/static/files/RFC2350.pdf

Chaudhary, S., Gkioulos, V., & Katsikas, S. (2022). Developing metrics to assess the effectiveness of cybersecurity awareness program. *Journal of Cybersecurity*, *8*(1), tyac006. https://doi.org/10.1093/cybsec/tyac006

Chen, K. Y. (2021). *A Systematic Approach for Cybersecurity Risk Management* [Massachusetts Institute of Technology]. https://dspace.mit.edu/handle/1721.1/139995

CISA. (2020). *Cyber Resilience Review (CRR) Resource Guide: Vulnerability Management*. https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf

CISA. (2024). *Traffic Light Protocol (TLP) Definitions and Usage*. https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

Deputi III, B. (2024). *Peraturan Deputi Bidang Keamanan Siber dan Sandi Pemerintahan dan Pembangunan Manusia Nomor 1 Tahun 2024 Tentang Pedoman Pembentukan Tim Tanggap Insiden Siber Sektor Pemerintahan*.

Direktorat Operasi Keamanan Siber. (2023). *Lanskap Keamanan Siber Indonesia 2023*. https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

FIRST. (2015). Common Vulnerability Scoring System v3.0: Specification Document. *Forum of Incident Response and Security Teams (FIRST)*, 1–21. https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf

FIRST. (2017). *Common Vulnerability Scoring System v3.0 Examples*. https://www.first.org/cvss/cvss-v30-examples_v1.5.pdf

FIRST. (2023). *CSIRT Services Framework v2.1*. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Foreman, P. (2019). *Vulnerability Management* (2nd ed.). Auerbach Publications. https://doi.org/10.1201/9780429289651

Gartner. (2020). *A Guidance Framework for Developing and Implementing Vulnerability Management*. https://www.gartner.com/en/documents/3747620

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, *57*, 710–715. https://doi.org/https://doi.org/10.1016/j.procs.2015.07.458

Government of South Australia. (2021). *Vulnerability Management and Patching Guideline (SACSF-G11.0)*. https://www.security.sa.gov.au/documents/documents/SACSF-G11.0-Vulnerability-management-and-Patching-Guideline.pdf

Guidelines for Cyber Security Incidents. (2024). https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents

Hanford, S., & Heitman, M. (2015). Common Vulnerability Scoring System v3 . 0 : User Guide. *FIRST-Forum of Incident Response and Security Teams*, 1–15. https://www.first.org/cvss/cvss-v30-user_guide_v1.5.pdf

Huawei. (2023). *Huawei Vulnerability Management White Paper 2023*.

IoT Security Foundation. (2021). *Vulnerability Disclosure Best Practice Guidelines, Release 2.0*. https://www.iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf

ISO. (2018). *ISO/IEC 29147:2018 Information technology – Security techniques – Vulnerability disclosure* (Issue ISO/IEC 29147:2018). https://www.iso.org/standard/72311.html

ISO. (2019). *ISO/IEC 30111:2019 Information technology – Security techniques – Vulnerability handling processes* (Issue ISO/IEC 30111:2019). https://www.iso.org/standard/69725.html

JPCERT/CC. (2024). *About JPCERT/CC*. https://www.jpcert.or.jp/english/about/

Kissoon, T. (2022). *Optimal Spending on Cybersecurity Measures: Risk Management*. Routledge. https://www.routledge.com/Optimal-Spending-on-Cybersecurity-Measures-Risk-Management/Kissoon/p/book/9781032061412

Knerler, K., Parker, I., & Zimmerman, C. (2022). *11 Strategies of a World-Class Cybersecurity Operations Center*.

Matwyshyn, A. M., Cui, A., Keromytis, A. D., & Stolfo, S. J. (2010). Ethics in security vulnerability research. *IEEE Security & Privacy*, *8*(2), 67–72. https://doi.org/10.1109/MSP.2010.67

Mohammed, A. H. Y., Dziyauddin, R. A., & Latiff, L. A. (2023). Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges. *International Journal of Advanced Computer Science and Applications*, *14*(1). https://doi.org/10.14569/IJACSA.2023.0140119

National Cyber Security Centre. (2022). *Vulnerability Disclosure Toolkit*. https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf

NIST. (2012a). *Computer Security Incident Handling Guide* (Issue SP 800-61 Revision 2). https://doi.org/10.6028/NIST.SP.800-61r2

NIST. (2012b). *Guide for Conducting Risk Assessments* (Issue NIST Special Publication 800-30 Revision 1). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

NIST. (2024). *National Vulnerability Database (NVD)*. https://nvd.nist.gov/

Office of the CISO. (2024). *Vulnerability management guidelines*.

OWASP Foundation. (2021). *OWASP Top Ten Web Application Security Risks*. https://owasp.org/Top10/

Pipyros, K. (2019). *A new systematic modelling methodology for improving cyber-attack evaluation on states' Critical Information Infrastructure (CII) Kosmas Pipyros*.

Presiden Indonesia. (2019). *Peraturan Presiden Nomor 71 tahun 2019 tentang Penyelenggaran Sistem dan Transaksi Elektronik*.

Recorded Future. (2022). *The Intelligence Handbook: A Roadmap for Building an Intelligence-Led Security Program* (4th ed.). Recorded Future.

Roytman, M., & Bellis, E. (2023). *Modern Vulnerability Management: Predictive Cybersecurity*. Artech. http://ieeexplore.ieee.org/document/10121000

Sarker, K. U., Yunus, F., & Deraman, A. (2023). Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and Scoring Methods. *Sustainability*, *15*(13). https://doi.org/10.3390/su151310471

Scarfone, K. A., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical Guide to Information Security Testing and Assessment* (Issues 800–115). https://doi.org/10.6028/NIST.SP.800-115

Scarfone, K., & Souppaya, M. (2022). *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*. https://doi.org/10.6028/NIST.SP.800-40r4

Swanagan, M. (2024, March 1). *Vulnerability & Patch Management Metrics: Top 10 KPIs*. https://purplesec.us/learn/vulnerability-management-metrics/

University of Toronto. (2024). *Vulnerability Management Guidelines*. https://security.utoronto.ca/wp-content/uploads/2024/01/vulnerability-management-guidelines-20240118.pdf

US-CERT. (2020). *US-CERT InfoSheet v2*. https://www.cisa.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf

2024