BAB VIII

Keamanan Informasi Nuklir

Intan Savitri & Wenseslaus Roland

A. Pendahuluan

Informasi dapat dilihat sebagai sumber daya strategis dan potensial yang bisa digunakan untuk menciptakan keunggulan kompetitif bagi suatu organisasi. Organisasi yang dapat mengelola dan memanfaatkan informasi dengan baik, diharapkan dapat menggali potensi dirinya secara maksimal dalam upaya meraih keunggulan di dalam persaingan. Negara sebagai suatu konteks organisasi dalam skala besar, juga membuat, memproses, menangani, dan menyimpan banyak jenis informasi. Beberapa informasi tersebut, seperti rahasia militer atau informasi pribadi warga, mungkin dianggap cukup sensitif sehingga memerlukan perlindungan khusus. Negara dapat menetapkan undang-undang keamanan informasi nasional yang mendefinisikan dan mengklasifikasikan informasi serta menetapkan persyaratan

Intan Savitri* & Wenseslaus Roland

* Badan Riset dan Inovasi Nasional, e-mail: intan.savitri@brin.go.id

Savitri, I., & Roland, W. (2024). Keamanan informasi nuklir. Dalam Antariksawan, A. R. (Ed.), *Memperkuat Keamanan Nuklir Untuk Meningkatkan Pemanfaatan Iptek Nuklir* (173–210). Penerbit BRIN. DOI: 10.55981/brin.760.c996, E-ISBN: 978-623-8372-75-1

perlindungan khusus, termasuk persyaratan untuk data dalam bentuk digital dan untuk sistem berbasis komputer terkait.

Indonesia telah memiliki Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) Nomor 11 Tahun 2008 (UU No. 11, 2008) dan versi revisi UU ITE Nomor 19 Tahun 2016 (UU No. 19, 2016). UU ITE memberikan perlindungan hukum untuk konten sistem elektronik dan transaksi elektronik. Namun, UU ini tidak mencakup aspek penting keamanan siber, seperti infrastruktur informasi dan jaringan, serta sumber daya manusia dengan keahlian di bidang keamanan siber (Anjani, 2021). Dalam UU ITE juga belum diatur mengenai serangan-serangan siber yang dapat mengganggu stabilitas keamanan dan pertahanan Indonesia (Setiyawan et al., 2020). Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 (Permenhan No. 82, 2014) menyediakan pedoman pertahanan siber untuk menghadapi ancaman siber terhadap keamanan nasional. Peraturan tersebut menjabarkan definisi keamanan siber, yang berbunyi "Keamanan siber nasional adalah segala upaya dalam rangka menjaga kerahasiaan, keutuhan, dan ketersediaan informasi serta seluruh sarana pendukungnya di tingkat nasional, yang bersifat lintas sektor". Tidak seperti UU ITE, peraturan ini mencakup infrastruktur penting, misalnya dari sistem keuangan dan transportasi sebagai objek keamanan siber. Namun, peraturan ini hanya berguna untuk mengembangkan kapasitas pertahanan siber militer (Anjani, 2021). Untuk ancaman siber non militer, khususnya ancaman terhadap infrastruktur penting lainnya, dapat mengacu pada Peraturan Presiden Nomor 82 tahun 2022 tentang Perlindungan Infrastuktur Informasi Vital (IIV) (Perpres No. 82, 2022). Tujuan diterbitkannya Perpres tersebut adalah untuk melindungi keberlangsungan penyelenggaraan IIV secara aman, andal, dan tepercaya; mencegah terjadinya gangguan, kerusakan, dan/atau kehancuran pada IIV akibat serangan siber, dan/atau ancaman/kerentanan lainnya; dan meningkatkan kesiapan dalam menghadapi insiden siber serta mempercepat pemulihan dari dampak insiden siber. Pada Perpres tersebut, IIV didefinisikan sebagai sistem elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, baik berdiri

sendiri maupun saling bergantung dengan sistem elektronik lainnya dalam menunjang sektor strategis. Jika terjadi gangguan, kerusakan, dan/atau kehancuran pada infrastruktur tersebut akan berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional. Berdasarkan definisi tersebut fasilitas nuklir dapat termasuk di dalamnya, tetapi tidak disebutkan secara eksplisit. Sektor IIV yang dimaksud pada Perpres tersebut meliputi administrasi pemerintahan, energi dan sumber daya mineral, transportasi, keuangan, kesehatan, teknologi informasi dan komunikasi, pangan, pertahanan, dan sektor lain yang ditetapkan presiden.

Selain merujuk pada peraturan terkait keamanan informasi yang telah diterbitkan oleh pemerintah Indonesia, keamanan informasi di fasilitas nuklir juga dapat merujuk pada pedoman yang dikeluarkan oleh Badan Tenaga Atom Internasional (International Atomic Energy Agency, IAEA). IAEA menerbitkan berbagai panduan dan pedoman serta rekomendasi terkait keamanan informasi karena hal tersebut merupakan ancaman bagi keselamatan dan keamanan fasilitas nuklir. Terlebih lagi, serangan siber pernah terjadi di beberapa fasilitas nuklir meski hal tersebut tidak menimbulkan kerusakan ataupun hingga menghentikan operasi fasilitas nuklir tersebut (Shalal, 2016).

Artikel *"Objective and Essential Elements of a State's Nuclear Security Regime: Nuclear Security Fundamentals"* dalam seri *Nuclear Security Series* (NSS) No. 20 berisi rekomendasi 12 elemen dasar (*essential elements*) untuk menjaga rezim keamanan nuklir, menekankan pentingnya keamanan informasi, termasuk keamanan komputer, dalam rezim keamanan nuklir (*nuclear security regime*) (IAEA, 2013). Dokumen tersebut juga menggarisbawahi pentingnya mengindentifikasi isu dan faktor yang dapat memengaruhi kapasitas dalam penyediaan keamanan nuklir yang memadai, termasuk keamanan komputer. Keamanan informasi sensitif juga merupakan komponen penting yang disebut dalam klausul Elemen Dasar 3, di antaranya menyatakan bahwa kerangka legislatif, peraturan, dan tindakan administratif terkait, harus ditetapkan untuk melindungi

kerahasiaan informasi sensitif dan untuk melindungi aset informasi sensitif. Keamanan informasi sensitif dan aset informasi sensitif mencakup di dalamnya perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi/aset tersebut.

Pada tahun 2016, semua negara pihak Konvensi Proteksi Fisik Material Nuklir (Convention on the Physical Protection on Nuclear Material, CPPNM) juga menyetujui secara konsensus amandemen CPPNM untuk memasukkan klausul perlindungan kerahasiaan informasi dalam Prinsip Fundamental L (IAEA, 2016). Adapun perlindungan terhadap sistem berbasis komputer (termasuk sistem instrumentasi dan kontrol) ditetapkan dalam Rekomendasi Keamanan Nuklir tentang Perlindungan Fisik Bahan Nuklir dan Fasilitas Nuklir (IAEA, 2011a). Paragraf 4.10 menyatakan bahwa:

"Sistem berbasis komputer yang digunakan untuk perlindungan fisik, keselamatan nuklir dan akuntansi, serta pengendalian bahan nuklir harus dilindungi dari hal yang membahayakan (misalnya serangan dunia maya, manipulasi, atau pemalsuan) yang dilakukan melalui penilaian ancaman ataupun melalui ancaman dasar desain (*design basis threat*/DBT)."

Selain beberapa pedoman di atas, Rekomendasi Keamanan Nuklir pada Bahan Radioaktif dan Fasilitas Terkait (IAEA, 2011b) serta Rekomendasi Keamanan Nuklir dan Bahan Radioaktif Lainnya di luar Kendali Regulasi (IAEA, 2011c) juga menekankan perlunya mencegah akses tidak sah ke informasi sensitif dan untuk melindunginya dari hal yang membahayakan.

B. Keterkaitan Informasi dan Sistem Berbasis Komputer pada Rezim Keamanan Nuklir

Informasi merupakan pengetahuan yang dapat berupa ide, konsep, proses, fakta, atau bahkan pola. Informasi dapat direkam secara fisik melalui media seperti kertas ataupun disimpan secara digital pada media optik atau magnetik, atau bahkan pada media penyimpanan awan (*cloud storage*).

Sistem berbasis komputer adalah teknologi yang dapat memproses, menghitung, mengomunikasikan, atau menyimpan informasi digital. Sistem tersebut dapat berupa desktop, laptop, tablet, *smart phone*, komputer *mainframe*, server, instrumentasi digital dan perangkat kontrol, pengontrol logika yang dapat diprogram (*programmable logic controller*, PLC), *printer*, ataupun perangkat jaringan. Sistem tersebut juga dapat mencakup layanan virtual, seperti komputasi awan atau mesin virtual. Sistem tersebut dapat berupa sebuah komponen tunggal atau berupa kumpulan aset digital.

Sistem berbasis komputer memainkan peranan penting dalam pembuatan, pengolahan dan pemrosesan, penyimpanan dan transmisi, serta penyebaran informasi. Bahkan di beberapa bidang, seperti perancangan dan simulasi, pemanfaatan kemampuan komputasi sistem berbasis komputer menjadi sesuatu yang mutlak. Hal ini didukung pula oleh evolusi teknologi di bidang komputasi dan komunikasi yang makin menguatkan peran sistem berbasis komputer dan dengan cepat menggantikan metode pengolahan informasi yang konvensional.

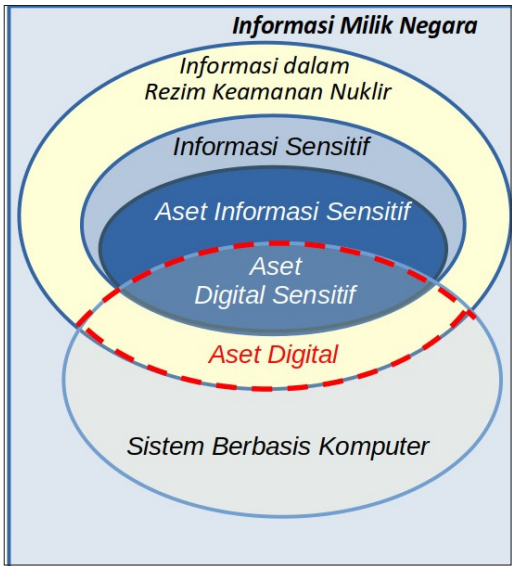
Sistem informasi berbasis komputer bisa menjamin konsistensi hasil pengolahan dan pemrosesan data tanpa memandang waktu dan lamanya komputasi berlangsung. Dengan demikian, kualitas hasil pengolahan data lebih andal dengan kualitas yang bisa diukur. Hasil pengolahan informasi yang cepat dan berkualitas akan membantu proses analisis suatu keadaan dan mempercepat pengambilan keputusan terhadap berbagai situasi, baik itu dalam simulasi maupun dalam keadaan riil.

Aset digital adalah sistem berbasis komputer (atau bagian dari sistem berbasis komputer) yang terkait dengan rezim keamanan nuklir. Istilah aset digital sensitif (*sensitive digital aset*, SDA) digunakan untuk mengidentifikasi aset informasi sensitif yang merupakan bagian dari sistem berbasis komputer. Aset informasi sensitif didefinisikan sebagai peralatan atau komponen yang digunakan untuk menyimpan, memproses, mengontrol, atau mengirimkan informasi sensitif.

Gambar 8.1 memperlihatkan keterkaitan antara aset informasi sensitif, sistem berbasis komputer, dan aset digital sensitif. Aset infor-

masi sensitif pada fasilitas nuklir dapat berupa rincian sistem proteksi fisik; sistem personel dan rencana; rincian jenis, jumlah, kualitas, dan lokasi bahan nuklir dan zat radioaktif lainnya yang ditempatkan di fasilitas; serta informasi transportasi, jadwal, dan keamanan untuk pergerakan bahan nuklir.

Aset informasi sensitif ini, termasuk yang dalam bentuk aset digital, perlu dilindungi dengan menerapkan prinsip-prinsip dasar keamanan informasi. Adapun yang dimaksud keamanan informasi di sini adalah sekumpulan metodologi, praktik, ataupun proses yang dirancang dan diterapkan untuk melindungi informasi atau data pribadi dari akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak sah. Keamanan informasi bertujuan untuk melindungi informasi pada berbagai tahap, baik itu saat penyimpanan, transfer, maupun penggunaannya.



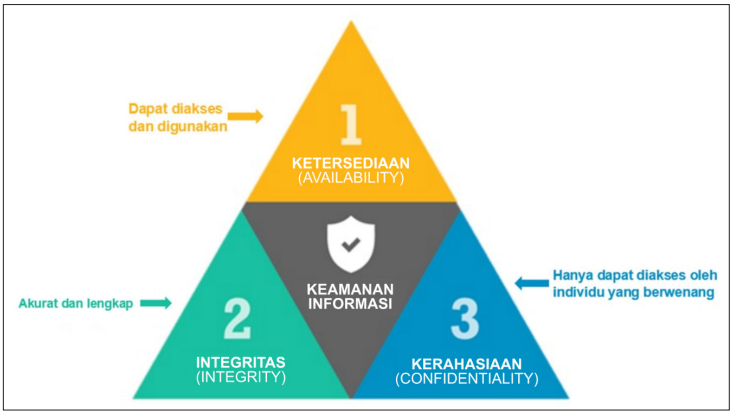
Sumber: IAEA (2021a)

Gambar 8. 1 Informasi dan Sistem Berbasis Komputer pada Rezim Keamanan Nuklir

Dalam konteks keamanan informasi, aset informasi mungkin memiliki satu atau lebih persyaratan keamanan. Tiga persyaratan keamanan informasi yang paling umum, dikenal dengan istilah triad CIA (*Confidentiality-Integrity-Availability*), seperti ditunjukkan pada Gambar 8.2 (Alexander & Panguluri, 2016). Triad CIA adalah model standar dalam keamanan informasi yang dirancang untuk mengatur dan mengevaluasi bagaimana informasi disimpan, dikirim, atau diproses. Setiap aspek yang ada di dalam triad CIA akan menjadi komponen penting dari keamanan informasi.

Confidentiality (kerahasiaan) mengartikan bahwa informasi hanya dapat diakses oleh individu yang berwenang. Guna menjaga kerahasiaan, perlu disusun langkah-langkah untuk menghentikan individu yang tidak berwenang mengakses informasi sensitif, dan perlu disusun kategorisasi terhadap informasi berdasarkan tingkat sensitivitasnya, serta penerapan perlindungan yang berbeda berdasarkan kategorisasi tersebut. Salah satu metode yang umum digunakan untuk memastikan kerahasiaan informasi adalah metode enkripsi.

Integrity (integritas) mengartikan bahwa informasi tersebut akurat dan lengkap. Integritas berkaitan dengan proses menjaga akurasi, konsistensi, dan kepercayaan informasi. Suatu informasi tidak boleh diubah (baik pada saat disimpan maupun saat dipindahkan) oleh orang yang tidak berwenang. Metode yang dapat digunakan untuk menjaga integritas, antara lain, penerapan izin akes file (file permissions) dan penerapan kontrol versi.



Sumber: IAEA (2021b)

Gambar 8.2 Triad CIA

Availability (ketersediaan) mengartikan bahwa individu yang berwenang dapat mengakses dan menggunakan informasi setiap saat. Untuk memastikan faktor ketersediaan, sistem yang terkait harus memiliki redudansi ataupun prosedur *failover. Failover* merupakan kemampuan suatu sistem untuk berpindah ke sistem cadangan jika sistem utama mengalami kegagalan.

Perlindungan keamanan terhadap informasi selama ini dilakukan dengan mengandalkan perlindungan fisik. Seiring dengan transformasi digital, perlindungan fisik semata tidak lagi mampu melindungi informasi. Oleh karena itu, perlu juga diperhatikan faktor terkait keamanan komputer. Keamanan komputer adalah aspek tertentu dari keamanan informasi yang berkaitan dengan perlindungan sistem berbasis komputer dari hal-hal berbahaya. Istilah keamanan teknologi informasi dan keamanan siber dapat dianggap sinonim dengan keamanan komputer. Keamanan komputer merupakan bagian dari keamanan informasi, sebagaimana dinyatakan dalam pedoman IAEA terkait Keamanan Informasi Nuklir (IAEA, 2015). Keamanan informasi dan keamanan komputer sering kali memiliki tujuan, metodologi, dan terminologi yang sama.

C. Ancaman dan Serangan Keamanan Informasi/ Komputer Nuklir

Sistem berbasis komputer memainkan peranan penting dalam semua aspek operasi yang aman dan selamat di fasilitas nuklir. Aspek operasi ini meliputi penggunaan, penyimpanan, pengangkutan bahan nuklir dan zat radioaktif lainnya, termasuk pemeliharaan sistem proteksi fisik, serta tindakan deteksi dan responsss terhadap bahan nuklir yang berada di luar pengawasan. Seiring kemajuan teknologi, penggunaan sistem berbasis komputer di semua aspek operasi tersebut tentunya akan meningkat. Hal ini juga dapat memicu peningkatan risiko dan ancaman keamanan siber. Mengingat adanya keterkaitan antara interkonektivitas jaringan komputer dengan aliran informasi, langkah-langkah keamanan komputer juga diperlukan untuk melindungi aset informasi sensitif dari ancaman yang dapat mengeksploitasi aset digital ataupun sistem berbasis komputer lainnya. Ancaman yang berhasil mengeksploitasi kelemahan sistem komputer dapat berubah menjadi serangan siber.

Serangan siber adalah serangan berbahaya yang dilakukan oleh individu atau organisasi terhadap suatu aset informasi sensitif dengan tujuan mengubah, menghalangi akses, atau menghancurkan target tertentu melalui tindakan atau akses tidak sah di dalam sistem yang rentan. Untuk memahami serangan siber, perlu juga diketahui ancaman siber yang mungkin terjadi. Ancaman siber berbeda dengan ancaman fisik yang dihadapi oleh fasilitas nuklir. Ancaman siber tidak dibatasi oleh lokasi, jumlah penyerang, ataupun batas fasilitas yang ditargetkan. Pemahaman tentang karakteristik ancaman serta skenario serangan siber dapat memberikan wawasan berharga tentang tindakan pencegahan yang dapat dilakukan. Ancaman siber dapat dikategorikan dengan beberapa cara. Berikut contoh pengkategorian ancaman siber berdasarkan aktor yang terlibat (IAEA, 2021c).

1) Ancaman Orang Dalam (*Insider Threat*)
   Salah satu ancaman yang paling kompleks adalah ancaman orang dalam. 'Orang dalam' adalah individu dengan akses resmi ke fasilitas/aktivitas tertentu. Orang dalam memiliki akses

ke informasi dan aset informasi sensitif. Hal ini memberikan keuntungan bagi mereka untuk melakukan tindakan tidak sah yang disengaja, yang dapat melibatkan bahan nuklir atau bahan radioaktif lainnya serta memiliki dampak yang merugikan bagi keamanan nuklir. Orang dalam juga dapat melakukan tindakan tersebut tanpa disadari dan tidak memiliki motivasi atau niat tertentu, tetapi hal tersebut dimanfaatkan oleh penyerang untuk mengambil keuntungan.

2) Ekstremis (*Extremist*)
Istilah ekstremisme mengacu pada kelompok yang melampaui norma dalam ekspresi politik atau sosial. Aktivitas yang dilakukan ekstremis telah melampaui perilaku yang diterima. Ekstremis dapat melakukan aksinya seorang diri ataupun bekerja sama dengan individu dengan pandangan yang sama dalam melakukan serangan siber terhadap target yang ditentukan. Aksi kolektif semacam ini biasanya tidak dikendalikan oleh seorang tokoh sentral dan bisa jadi tidak beroperasi dengan aturan keterlibatan tertentu.

3) Peretas Rekreasi (*Recreational Hacker*)
Peretas rekreasi dapat berupa individu atau kelompok yang dimotivasi oleh ketenaran atau kemasyhuran, dan biasanya tidak memiliki keinginan untuk menimbulkan kerusakan atau keuntungan secara finansial. Aksi yang mereka lakukan mungkin tidak ditargetkan spesifik ke fasilitas nuklir, tetapi secara tidak disengaja berdampak terhadap fasilitas tersebut. Sebagai contoh, sistem kontrol di fasilitas nuklir terinfeksi virus umum yang berasal dari perangkat/media portabel yang tidak aman dan disambungkan ke sistem kontrol tersebut.

4) Kejahatan Terorganisir (*Organized Crime*)
Kejahatan terorganisir biasanya mengembangkan serangan siber yang sangat canggih dan ditargetkan terhadap berbagai sektor industri. Tujuannya adalah keuntungan finansial yang mungkin didapat secara langsung melalui pencurian uang atau secara tidak langsung dari penjualan data curian atau penjualan informasi yang dapat mengarah ke ancaman lain.

5) Pelaku Negara (*Nation State*)
Pelaku negara sering kali merepresentasikan ancaman yang sangat canggih dan gigih. Motivasi dan tujuan serangan semacam ini biasanya terbatas pada pengumpulan informasi dan sering kali terikat oleh aturan keterlibatan yang terstruktur.

6) Teroris (*Terrorist*)
Serangan siber di masa lalu yang dikaitkan dengan teroris, sebagian besar terdiri dari upaya sederhana seperti *spamming* email, serangan penolakan layanan (*denial of service*/DdoS), atau perusakan situs web. Namun, saat ini serangan yang dilakukan telah meningkat seiring dengan peningkatan kemampuan teknis untuk melakukan serangan berbasis jaringan. Kemampuan teknis ini mungkin muncul dari keahlian internal atau dari mempekerjakan peretas (*hacker*). Target teroris bisa berupa sabotase terhadap infrastruktur penting, seperti pembangkit listrik tenaga nuklir, bisa juga target untuk memperoleh bahan nuklir dan bahan radioaktif lainnya.

Selain kategori ancaman siber, penting juga untuk mengetahui karakteristik serangan guna membangun tindakan pencegahan, deteksi, mitigasi, dan responsss. Berikut beberapa contoh karakteristik serangan (IAEA, 2021c).

1) Serangan NonTarget (*NonTargeted Attack*)
Beberapa ancaman yang telah dijelaskan sebelumnya, melakukan aksi serangan terhadap target keamanan nuklir tertentu. Namun, serangan yang tidak ditargetkan juga dapat terjadi, misalnya kode berbahaya yang secara tidak sengaja dimasukkan ke dalam sistem dan jaringan berbasis komputer, yang dapat berdampak buruk pada keamanan nuklir. Sebagai contoh, sistem kontrol di fasilitas nuklir yang terinfeksi virus karena manajemen media portabel yang tidak aman.

2) Serangan Gigih (*Persistent Attacks*)
Serangan siber dapat berdampak langsung ataupun berupa bagian dari serangan terus-menerus yang dilakukan terhadap

fasilitas atau organisasi yang dampaknya tidak langsung terlihat. Serangan ini bisa dimulai dari terinfeksinya suatu sistem berbasis komputer yang dilanjutkan dengan pengumpulan informasi yang berkelanjutan. Aksi dari serangan ini bisa berdampak langsung atau bertujuan untuk membangun *backdoor* yang dapat digunakan untuk serangan di masa depan.

3) Serangan Campuran (*Blended Attacks*)
Serangan campuran merupakan perpaduan antara serangan fisik dengan serangan siber. Sebagai contoh, sistem kontrol akses fisik dapat disusupi oleh serangan siber sehingga memungkinkan masuknya individu yang tidak berwenang secara fisik.

Tabel 8.1 dan Tabel 8.2 menggambarkan kemungkinan serangkaian profil penyerang. Tabel 8.1 berfokus pada ancaman orang dalam, sedangkan Tabel 8.2 mengidentifikasi kemungkinan ancaman eksternal. Tabel 8.1 dan 8.2 menampilkan keterkaitan tipe umum penyerang dengan sumber daya penyerang, rentang waktu serangan, alat yang mungkin digunakan, dan motivasi penyerang.

Tabel 8.1 Ancaman Orang Dalam

Ancaman	Sumber Daya	Waktu	Taktik	Motivasi	Niat
Agen rahasia *(Covert agent)*	• Memfasilitasi 'rekayasa sosial' • Akses sistem pada tingkat tertentu • Tersedia dokumentasi dan keahlian sistem	Bervariasi, tetapi umumnya tidak dapat mengalokasikan waktu lama di luar jam kerja	Memiliki akses dan *password*, memiliki pengetahuan tentang pemrograman dan arsitektur sistem, kemungkinan dapat menanamkan backdoor/trojan, kemungkinan memiliki dukungan ahli eksternal	Politik, finansial, ideologi	Pencurian informasi bisnis, rahasia teknologi, sabotase informasi pribadi
Orang dalam yang dipaksa (Coerced insider)	• Memfasilitasi 'rekayasa sosial' • Akses sistem pada tingkat tertentu • Tersedia dokumentasi dan keahlian sistem	Bervariasi, tetapi umumnya tidak dapat mengalokasikan waktu lama di luar jam kerja	Memiliki akses dan *password*, memiliki pengetahuan tentang pemrograman dan arsitektur sistem, kemungkinan dapat menanamkan backdoor/trojan, kemungkinan memiliki dukungan ahli eksternal	Pribadi	Pencurian informasi bisnis, rahasia teknologi, sabotase informasi pribadi
Orang dalam tanpa disadari (Unwitting insider)	• Akses sistem terkait fungsi kerja biasa	–	Tanpa disadari menyediakan akses internal untuk musuh	Tidak dibutuhkan motivasi	–

Ancaman	Sumber Daya	Waktu	Taktik	Motivasi	Niat
Karyawan/pengguna sistem yang tidak puas					
Karyawan-Pengguna komputer nonteknis	• Sumber daya sedang/kuat • Akses sistem pada tingkat tertentu • Dokumentasi dan keahlian sistem tersedia untuk bisnis dan sistem operasi tertentu	Bervariasi, tetapi umumnya tidak dapat menghabiskan waktu berjam-jam	Memiliki akses dan *password*, memiliki pengetahuan tentang pemrograman dan arsitektur sistem, memiliki kemampuan untuk memasukkan alat atau skrip 'kiddie' (berpotensi lebih rumit jika mereka memiliki keterampilan komputer tertentu)	Pribadi, finansial	Balas dendam, pencurian informasi bisnis, mempermalukan majikan/karyawan lain, merendahkan citra atau kepercayaan publik
Karyawan-Pengguna komputer teknis, administrator, pengembang	• Akses dan otoritas komputer tingkat tinggi • Hak akses jarak jauh	Banyak waktu	–	Pribadi, finansial	–
Pegawai kontrak-Pihak ketiga	• Akses lokal dan remote • Terkait fungsi dukungan yang dikelola saat ini	Bervariasi	Penyusupan dalam elemen rantai pasokan pada elemen yang telah terkompromi, penyusupan melalui media seluler atau koneksi jarak jauh	Pribadi	Balas dendam, pencurian informasi bisnis, mempermalukan majikan/karyawan lain, merendahkan citra atau kepercayaan publik

Tabel 8.2 Ancaman Dari Luar

Ancaman	Sumber Daya	Waktu	Taktik	Motivasi	Niat
Serangan nontarget (*Nontargeted attack*)	Kemampuan bervariasi	Bervariasi	Tidak ada penargetan khusus, umumnya mengandalkan proses dan kerentanan teknologi informasi yang normal, termasuk rekayasa sosial	pribadi—kesenangan, status	Ketenaran, perhatian media, mencari peluang
Ekstremis (*Extremist*)	• Keterampilan yang bervariasi, tetapi umumnya terbatas • Sedikit pengetahuan tentang sistem di luar informasi publik	Waktu terbatas, kegiatan terkait dengan peristiwa saat ini atau baru-baru ini	• Aktivitas peretasan yang dilakukan individu atau kelompok kecil • Distribusi alat untuk penggunaan yang lebih luas	Memberikan efek politik	Perhatian media, merendahkan citra atau kepercayaan publik
Peretas rekreasi (*Recreational hacker*)	• Keterampilan yang bervariasi, tetapi umumnya terbatas • Sedikit pengetahuan tentang sistem di luar informasi publik	Banyak waktu, tidak terlalu sabar	Menggunakan skrip dan alat yang tersedia secara umum, tetapi dimungkinkan pengembangan alat	pribadi— kesenangan, status	• Mencari peluang • Eksploitasi peluang yang tersedia

Ancaman	Sumber Daya	Waktu	Taktik	Motivasi	Niat
Kejahatan terorganisir (*Organized crime)*	• Sumber daya yang kuat • Karyawan dengan keahlian khusus	Bervariasi, tetapi kebanyakan jangka pendek	• Skrip, alat buatan sendiri • Mungkin mempekerjakan *hacker* sewaan • Mungkin mempekerjakan mantan/karyawan saat ini • Rekayasa sosial	Pemerasan mengejar keuntungan finansial, mempermaikan ketakutan akan dijualnya informasi bisnis	Pencurian material, pencurian informasi sensitif, penjualan informasi atau akses
Pelaku negara (*Nation state)*	Bervariasi, tetapi mampu mendukung serangan berkelanjutan	Bervariasi, tetapi mampu mendukung serangan berkelanjutan	• Alat canggih • Mungkin mempekerjakan mantan/karyawan saat ini • Rekayasa sosial	• Politik • Koleksi intelijen • Membangun jalur akses untuk tindakan selanjutnya	Pencurian teknologi, pengintaian untuk serangan di masa depan, sabotase

Ancaman	Sumber Daya	Waktu	Taktik	Motivasi	Niat
Teroris (*Terrorist)*	• Keterampilan yang bervariasi • Kemungkinan pelatihan/pengalaman pengoperasian pada sistem • Kemungkinan infiltrasi dengan agen rahasia • Potensi untuk didanai dengan baik • Keterampilan yang berkembang	Banyak waktu, sangat sabar	• Skrip, alat buatan sendiri • Mungkin mempekerjakan peretas sewaan • Mungkin mempekerjakan mantan/karyawan saat ini • Rekayasa sosial	• Koleksi intelijen • Membangun jalur akses untuk tindakan selanjutnya • Kekacauan • Pembalasan dendam • Memengaruhi opini publik (ketakutan)	Dukungan untuk serangan campuran, pengintaian untuk serangan di masa depan, sabotase pencurian material

Sumber: IAEA (2021c)

Ancaman dan serangan siber pada fasilitas nuklir dapat terjadi, baik pada lingkungan teknologi informasi (*information Technology*, IT) maupun lingkungan teknologi operasional (*operational technology*, OT). Lingkungan IT berkaitan dengan sistem berbasis komputer yang menyimpan, mengambil, mengirimkan, dan memanipulasi informasi digital. Perangkat pada lingkungan IT dapat berupa komputer desktop, komputer *mainframe*, server, perangkat jaringan, atau bahkan komponen kecil seperti *programmable logic controllers* (PLC). Lingkungan OT berkaitan dengan perangkat yang memantau, mengelola, mengontrol, dan memanipulasi proses fisik dunia nyata. Perangkat tersebut dapat berupa perangkat analog ataupun digital. OT memiliki beberapa sinonim, tergantung pada industri di mana OT diterapkan. Pada industri infrastruktur kritis, OT dikenal dengan istilah sistem kontrol industri (*industrial control systems*, ICS). Sementara pada industri nuklir, OT dikenal dengan istilah sistem instrumentasi dan kontrol (*instrumentation and control systems*, I&C systems). Ketika OT digunakan untuk memantau proses jarak jauh secara geografis, OT dikenal dengan istilah sistem *supervisory control and data acquisition* (SCADA).

Terdapat sejumlah perbedaan antara IT dan OT yang harus dipahami guna melindungi kedua lingkungan ini. Tidak semua strategi pengamanan pada lingkungan IT dapat diimplemantasikan pada lingkungan OT (Kim et al., 2020). Dalam melihat lingkungan OT, sudut pandang teknis harus dipertimbangkan guna menentukan kerentanan yang mungkin timbul sehingga kontrol keamanan teknis dapat diterapkan. Tabel 8.3 memperlihatkan perbandingan antara lingkungan IT dan lingkungan OT.

Tabel 8.3 Perbandingan Lingkungan IT dan Lingkungan OT

Variabel	Lingkungan IT	Lingkungan OT
Ketersediaan	Memungkinkan adanya *downtime*	Tidak memungkinkan adanya *downtime*
Waktu kritis	Umumnya dapat menerima penundaan	Kritis

Variabel	Lingkungan IT	Lingkungan OT
Dukungan teknologi	2–3 tahun	Lebih dari 20 tahun
Pembaharuan keamanan	Reguler/terjadwal	Tidak umum diterapkan
Kesadaran keamanan	Berjalan baik, disektor publik ataupun swasta	Lemah, kecuali pada pengamanan fisik
Antivirus	Sangat umum, mudah digunakan dan diperbarui	Jarang dan mungkin sulit untuk diterapkan
Outsourcing	Umum/banyak digunakan	Langka
Tanggapan insiden	Didefinisikan dengan baik dan diterapkan	Tidak biasa
Pengujian/audit keamanan	Dijadwalkan dan dilaksanakan	Tidak mapan

Sumber: IAEA (2021b)

Sistem instrumentasi dan kendali (SIK) memiliki peranan penting dalam memastikan aspek keselamatan pada fasilitas nuklir. Dalam perancangan SIK di fasilitas nuklir pada masa lampau, faktor keamanan komputer tidak menjadi pertimbangan yang penting. Hal ini disebabkan karena SIK bersifat analog, dapat berdiri sendiri, terisolasi dan terpisah dari sistem lain, serta hampir tidak adanya komunikasi interaktif dengan jaringan/sistem eksternal yang membuat SIK dianggap kebal terhadap serangan siber.

Namun, fasilitas nuklir baru yang lebih modern dirancang dengan memanfaatkan SIK digital yang terintegrasi sehingga secara efisien dan simultan dapat menangani pemrosesan data dalam jumlah besar dan membutuhkan lebih sedikit campur tangan manusia dibandingkan SIK sebelumnya. Tindakan operator, seperti pemantauan panel berbasis kabel dan kontrol manual sakelar, telah diganti dengan visualisasi berbasis komputer dan aktuasi otomatis. Hal ini mendukung tanggapan yang lebih cepat dalam pengoperasian pada ruang kontrol serta mengurangi sumber daya manusia dan biaya (Park & Suh, 2014). Transisi ke teknologi digital telah mengubah sifat SIK di fasilitas nuklir sehingga memungkinkan sistem tersebut

dapat diprogram ulang dan berbeda secara fungsional serta memiliki interkoneksi dengan sistem eksternal, baik secara jarak jauh maupun lokal. Penerapan teknologi digital dalam SIK dapat membuat sistem ini rentan terhadap serangan siber.

Serangan siber pada SIK dapat membahayakan keselamatan dan keamanan fasilitas nuklir. Serangan ini dapat berkontribusi pada tindakan sabotase atau membantu pemindahan secara tidak sah. Efek serangan siber pada sistem I&C yang terkait dengan keselamatan dapat mengakibatkan berbagai konsekuensi, seperti hilangnya kontrol proses atau timbulnya konsekuensi radiologis yang tidak dapat diterima. Serangan siber yang memengaruhi SIK juga dapat merusak kepercayaan publik terhadap keselamatan dan keamanan fasilitas nuklir. Secara umum, serangan siber pada fasilitas nuklir dapat mengakibatkan hal-hal berikut:

1) kerusakan fisik pada fasilitas dan/atau lumpuhnya sistem keamanan atau keselamatannya (melalui sabotase);
2) didapatkannya akses tidak sah ke informasi nuklir sensitif yang dapat menyebabkan perubahan, kehilangan, serta penolakan akses ke informasi sensitif tersebut;
3) turunnya kemampuan untuk mencegah, mendeteksi, dan menanggapi peristiwa keamanan nuklir; dan
4) keberhasilan dalam memindahkan bahan nuklir tanpa izin.

Diperlukan kegigihan dalam menilai ancaman dan serangan yang terjadi saat ini karena penyerang, alat, taktik, dan target selalu berubah secara dinamis. Faktor-faktor yang memengaruhi perubahan tersebut, yaitu (IAEA, 2021c):

1) peningkatan jumlah musuh yang memiliki kemampuan untuk melakukan serangan siber;
2) peningkatan jumlah individu atau kelompok yang menawarkan layanan untuk membantu melakukan serangan siber. Hal ini dapat membantu penyerang yang sebelumnya tidak memiliki keterampilan.

3) teknik yang makin canggih, yang digunakan untuk serangan siber, membuat deteksi dan responsss menjadi lebih sulit;
4) peningkatan penggunaan rekayasa sosial dalam serangan siber, termasuk teknik '*spear phishing*' dan '*watering hole*';
5) peningkatan kemampuan musuh dalam menemukan dan mengeksploitasi kerentanan dalam sistem kontrol industri;
6) penyebaran *ransomware*;
7) kesulitan dalam mengamankan rantai pasokan dari serangan siber.

Mempertahankan keamanan komputer yang efektif di fasilitas nuklir merupakan tantangan yang signifikan karena ancaman yang substansial terus muncul dan berkembang dengan pesat (Department for Business, Energy & Industrial Strategy [BEIS], 2022). Banyak elemen penting dari rezim keamanan nuklir bergantung pada sistem berbasis komputer. Oleh karena itu, keamanan komputer sangat penting di fasilitas nuklir untuk melindungi keamanan dan keselamatan nuklir. Hal ini harus didukung oleh program keamanan komputer yang andal.

D. Program Keamanan Komputer

Program keamanan komputer adalah sebuah rencana untuk mengimplementasikan strategi keamanan komputer yang menetapkan peran, tanggung jawab, dan prosedur organisasi. Program keamanan komputer harus menentukan dan merinci cara untuk mencapai tujuan keamanan komputer. Program ini juga merupakan bagian dari program keamanan secara keseluruhan.

Program keamanan komputer harus menjelaskan keamanan komputer dalam organisasi, terkait kerentanan, tindakan perlindungan, analisis konsekuensi, dan tindakan mitigasi. Program keamanan komputer juga harus dapat mengidentifikasi dan mempertahankan tingkat risiko yang diterima akibat dari serangan siber yang muncul dan juga dapat memfasilitasi pemulihan ke keadaan operasional yang

aman. Isi dari program keamanan komputer minimal harus mencakup organisasi dan tanggung jawab, manajemen aset digital, penilaian risiko, kerentanan dan kepatuhan, desain keamanan sistem, prosedur keamanan operasional, dan manajemen personalia (IAEA, 2021c).

Program keamanan komputer harus memuat langkah-langkah keamanan komputer. Langkah-langkah keamanan komputer meliputi fungsi pencegahan, deteksi, penundaan, responsss, dan mitigasi. Langkah ini juga harus memastikan bahwa kejadian yang muncul tidak mengarah pada penurunan keamanan komputer yang mengakibatkan peningkatan kerentanan terhadap serangan siber. Terdapat tiga kontrol keamanan komputer, yaitu kontrol administratif, fisik, dan teknis (IAEA, 2018; IAEA, 2021c).

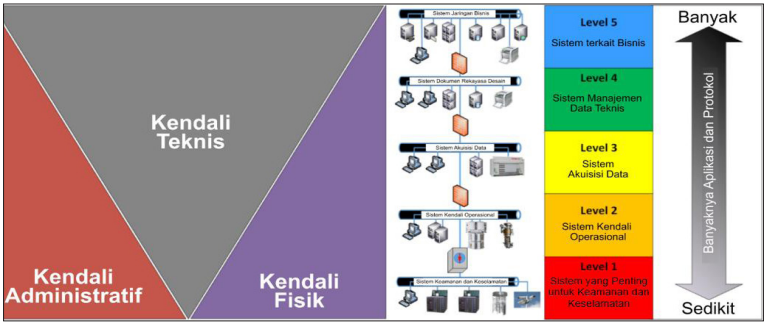
Kontrol administratif dapat berupa kebijakan, prosedur, dan praktik yang dirancang untuk melindungi sistem komputer melalui tindakan dan perilaku personel. Kontrol ini mencakup tindakan operasional dan manajemen, dan biasanya bersifat direktif, yang menetapkan apa yang boleh dan tidak boleh dilakukan oleh karyawan maupun personel pihak ketiga. Kontrol ini juga mencakup tindakan yang memengaruhi seperti penerapan budaya keamanan yang kuat.

Kontrol fisik dapat berupa penghalang fisik untuk perlindungan komputer serta aset pendukung dari kerusakan fisik dan akses fisik yang tidak sah. Hal-hal yang termasuk dalam langkah-langkah pengendalian fisik berupa personel keamanan, penghalang seperti kunci, pagar, gerbang, sistem proteksi fisik, serta ruang isolasi.

Kontrol teknis dapat berupa solusi perangkat keras/perangkat lunak komputer untuk perlindungan, deteksi, mitigasi, dan pemulihan dari penyusupan atau tindakan berbahaya. Contoh kontrol teknis, yaitu penerapan *firewall, intrusion detection system* (IDS), perangkat lunak antivirus, maupun berupa kontrol akses.

Ketiga kontrol ini harus diterapkan bersama-sama untuk melindungi keamanan komputer. Gambar 8.3 mengilustrasikan penerapan ketiga kontrol dalam sistem berbasis komputer. Penerapan satu kontrol pada satu waktu, dan mengabaikan kontrol yang lain, tidak dapat dilakukan. Pada fasilitas nuklir, kemampuan untuk

menerapkan kontrol teknis pada tingkat keamanan yang lebih rendah, misalnya pada sistem penting terkait keselamatan dan keamanan, cenderung lebih terbatas. Pada tingkat keamanan yang lebih rendah membutuhkan ketergantungan yang lebih besar pada kontrol fisik dan administratif.



Sumber: IAEA (2021b)

Gambar 8.3 Penerapan Kontrol Administratif, Fisik, dan Teknis pada Pendekatan Bertingkat

Pada Gambar 8.3 diperlihatkan sistem dengan tingkat keamanan pertama, yaitu sistem yang paling dijaga keamanannya, yakni sistem keamanan dan keselamatan. Dalam sistem ini, kontrol teknis yang diterapkan terbatas. Pada sistem ini, tidak dapat dipasang *firewall* ataupun dilakukan enkripsi komunikasi data. Bila hal tersebut dilakukan, dapat memperlambat sistem atau bahkan memunculkan kegagalan. Namun, sebagai kompensasinya, dapat diterapkan kontrol fisik dan administratif yang lebih besar, misalnya sistem diletakkan di area terbatas dan hanya orang-orang tertentu yang dapat mengakses ruangan.

Langkah-langkah keamanan komputer dalam program keamanan komputer harus didasarkan pada pendekatan bertingkat (*graded approach*), di mana langkah-langkah keamanan diterapkan secara proporsional terhadap potensi dampak serangan siber. Salah satu implementasi praktis dari pendekatan bertingkat adalah dengan membagi sistem berbasis komputer ke dalam beberapa zona. Pada tiap zona, langkah-langkah keamanan komputer diterapkan secara

berjenjang. Tabel 8.4 memperlihatkan contoh penerapan tingkat dan zona keamanan komputer pada ruang kendali utama di fasilitas nuklir.

Tabel 8.4 Contoh Penerapan Tingkat dan Zona Keamanan Komputer

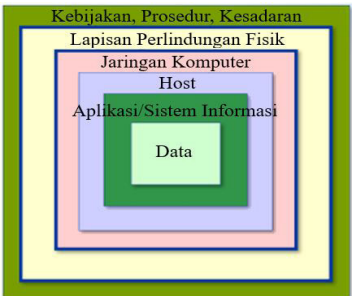
Sistem	Fungsi Utama	Tingkat	Batas Logis	Batas Fisik
Instrumen & kontrol sistem proteksi reaktor	Mencegah kondisi kecelakaan	1	• Jaringan internal khusus dipisahkan menggunakan *data diode*. • Tidak ada konektivitas jaringan eksternal.	• Peralatan diletakkan pada satu area vital saja. • Alat pengaman komputer (*data diode*) diletakkan pada area vital.
Instrumen & kontrol sistem pembatasan reaktor	Kontrol reaktivitas	2	Jaringan khusus dipisahkan menggunakan *data diode*, *firewall*, atau perangkat keamanan lainnya.	• Peralatan diletakkan pada satu atau lebih area vital. • Kabel jaringan, peralatan, atau perutean di luar area vital secara fisik diperketat keamanannya.
Instrumen & kontrol yang memproses sistem informasi	Memberikan alarm dan pemberitahuan kepada operator tentang lingkungan dan status fasilitas	3	• Jaringan yang saling terhubung dengan *human machine interface* (HMI). • Catatan: bisa berupa konsol HMI ruang kontrol utama yang terpisah/ tambahan	Peralatan dan jaringan diletakkan pada kawasan terlindungi dan/ atau kawasan vital

Sistem	Fungsi Utama	Tingkat	Batas Logis	Batas Fisik
Instrumen & kontrol sistem automasi operasional	Kontrol keseimbangan dari sistem fasilitas reaktor	3	• Jaringan yang saling terhubung dengan HMI. • Catatan: bisa berupa konsol HMI ruang kontrol utama yang terpisah/ tambahan atau digabungkan dengan instrumen dan kontrol yang memproses sistem informasi	Peralatan dan jaringan diletakkan pada kawasan terlindungi dan/ atau kawasan vital
IT perkantoran	Melakukan fungsi personalia	4	Tidak ada koneksi logis (antarmuka kabel, nirkabel, atau portabel) yang diizinkan dengan sistem pada tingkat 1, 2, atau 3	Diizinkan di area akses terbatas, area terlindungi, dan area vital
Sistem telekomunikasi	Panggilan ke pasukan responsss atau lembaga eksternal lainnya sesuai kebutuhan	4	Tidak ada koneksi logis (antarmuka kabel, nirkabel, atau portabel) yang diizinkan dengan sistem pada tingkat 1, 2, atau 3	Diizinkan di semua lokasi yang diperlukan untuk kepentingan operator

Sistem	Fungsi Utama	Tingkat	Batas Logis	Batas Fisik
Perangkat IT/ seluler pribadi	Tidak di-perlukan—hanya pengecualian	5	• Hanya diper-bolehkan di jaringan tingkat 5. • Tidak ada kedekatan dengan zona mana pun yang ditetapkan sebagai zona tingkat 1, 2 atau 3	Tidak diperbolehkan pada area vital

Sumber: IAEA (2021a)

Program keamanan komputer dapat menggabungkan pendekatan bertingkat dengan pertahanan berlapis (*defense in depth*). Pada pertahanan berlapis, lapisan pertahanan diimplementasikan pada berbagai tingkat arsitektur komputer dan dikombinasikan dengan kontrol teknis dan administratif. Dalam setiap langkah pengamanan pasti akan selalu ada kelemahan, tetapi dengan pertahanan berlapis dapat menciptakan perlindungan yang efektif karena perlindungan pada satu lapisan dapat menutupi kelemahan pada lapisan lain. Gambar 8.4 memperlihatkan pertahanan berlapis yang diterapkan pada sistem berbasis komputer.



Sumber: IAEA (2021b)

Gambar 8.4 Pertahan Berlapis Sistem Berbasis Komputer

Program keamanan komputer harus memuat dokumen terkait elemen dan tindakan yang direkomendasikan untuk mempertahankan keamanan komputer sebagai bagian dari rezim keamanan nuklir (IAEA, 2021c). Hal ini mencakup beberapa hal yang akan dijelaskan sebagai berikut.

1. Budaya keamanan

Orang dan proses sering menjadi faktor kunci dalam pengamanan sistem berbasis komputer. Kesalahan manusia (*human error*) adalah salah satu kontributor terbesar insiden keamanan komputer. Budaya keamanan harus mendukung karyawan dalam mengenali dan melaporkan perilaku yang tidak biasa dari sistem berbasis komputer, atau orang yang menggunakannya. Keamanan komputer harus dipromosikan sebagai komponen penting dari budaya keamanan nuklir melalui komitmen eksplisit dari manajemen senior dan melalui peningkatan kesadaran dan pelatihan. Program keamanan komputer harus mencakup kegiatan yang memperkuat budaya keamanan nuklir.

2. Pelatihan

Organisasi harus menetapkan program pelatihan untuk semua karyawan dan juga pihak ketiga tentang keamanan komputer. Program pelatihan harus mencakup kegiatan untuk meningkatkan kesadaran serta mengembangkan kompetensi dan keterampilan. Karyawan harus waspada terhadap risiko keamanan dan keselamatan nuklir terkait dengan potensi serangan siber yang mungkin terjadi pada fasilitas nuklir.

3. Rencana kontingensi dan responsss

Program keamanan komputer harus mencakup rencana darurat untuk mengatasi serangan siber. Rencana ini harus memperhitungkan kemungkinan serangan orang dalam dan juga serangan campuran. Rencana kontingensi harus mengidentifikasi jenis insiden keamanan komputer tertentu dan tanggapan yang diperlukan untuk mengatasi insiden ini.

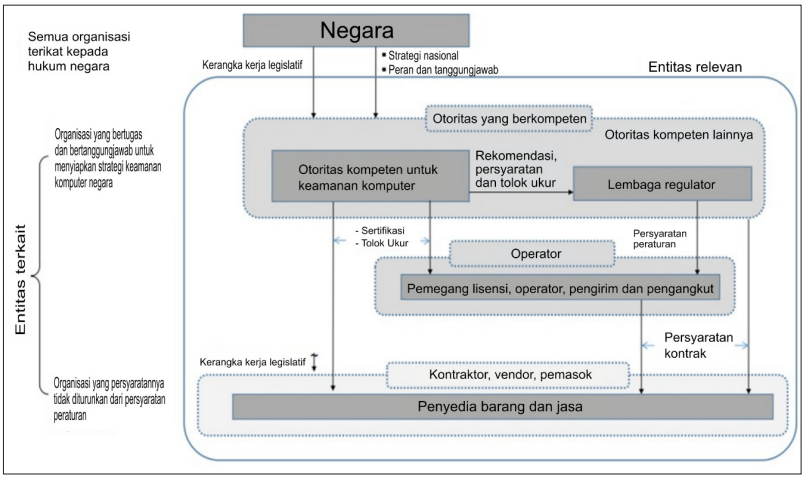
4. Jaminan keamanan komputer

Organisasi harus memastikan bahwa sistem manajemen mencakup sarana yang efektif untuk memberikan jaminan bahwa persyaratan

keamanan komputer terpenuhi, termasuk dalam rantai pasokan. Organisasi juga harus memastikan bahwa sumber daya yang ditugaskan untuk keamanan komputer sudah sesuai dan proporsional dengan tingkat ancaman yang diidentifikasi dalam penilaian ancaman. Inspeksi atau penilaian untuk memverifikasi kepatuhan terhadap persyaratan keamanan nuklir mencakup evaluasi langkah-langkah keamanan komputer.

E. Peran dan Tanggung Jawab Berbagai Institusi dan Individu

Guna mengimplementasikan, memelihara, dan mempertahankan keamanan komputer yang efektif dan andal, dibutuhkan dukungan dari berbagai pihak yang kompeten dan dapat dipercaya. Gambar 8.5 memperlihatkan berbagai pihak yang terlibat serta peran dan tanggung jawabnya. Negara sebagai otoritas tertinggi harus memastikan bahwa keamanan komputer ditangani dengan tepat dalam kerangka kerja legislatif dan peraturan dapat diterapkan dengan konsisten. Dalam menunjang fungsi ini, negara telah menerbitkan beberapa regulasi yaitu UU ITE No. 11 Tahun 2008 yang kemudian di revisi menjadi UU ITE No. 19 Tahun 2016, Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, dan yang terbaru adalah Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi V



Sumber: IAEA (2021b)

Gambar 8.5 Pihak yang Bertanggung Jawab dalam Keamanan Komputer

Selain dukungan regulasi, negara juga harus menunjuk otoritas yang berkompeten sebagai penanggung jawab utama untuk pengawasan dan penegakan hukum keamanan komputer. Pada Gambar 8.5 diperlihatkan dua otoritas yang berkompeten, yaitu otoritas kompeten untuk keamanan komputer dan lembaga regulator. Di Indonesia, otoritas kompeten keamanan komputer ditangani oleh Badan Siber dan Sandi Negara (BSSN), sementara lembaga regulator terkait fasilitas nuklir ditangani oleh Badan Pengawas Tenaga Nuklir (BAPETEN).

BSSN baru didirikan pada tahun 2017. Namun, tugas pengamanan informasi dan sandi nasional bukanlah tugas baru. Tugas ini sebelumnya diemban oleh Lembaga Sandi Negara dan Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika. Melalui Peraturan Presiden No. 53 Tahun 2017, kedua lembaga tersebut dilebur menjadi BSSN. Perpres ini kemudian dicabut dan digantikan dengan Peraturan Presiden No. 28 Tahun 2021 yang merupakan dasar hukum dari BSSN saat ini. BSSN bertugas melaksanakan keamanan siber secara efektif dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait keamanan siber. Dalam menjalankan tugas penjagaan keamanan siber

tersebut, BSSN berkoordinasi dengan penyelenggara fungsi siber lainnya, yaitu dengan Kementerian Luar Negeri Republik Indonesia sebagai penyelenggara fungsi diplomasi siber, dengan Kementerian Pertahanan Republik Indonesia dan Tentara Nasional Indonesia untuk fungsi siber pertahanan, dengan Kepolisian Republik Indonesia untuk kejahatan siber, dan dengan Kementerian Komunikasi dan Informatika Republik Indonesia untuk fungsi penyaringan internet (Chryshna, 2021).

BAPETEN sebagai lembaga regulator terkait fasilitas nuklir yang ditetapkan melalui Undang-undang Nomor 10 Tahun 1997 mempunyai fungsi pengawasan terhadap penggunaan tenaga nuklir, yang meliputi perizinan, inspeksi, dan penegakan peraturan untuk menjamin kepatuhan pengguna tenaga nuklir terhadap peraturan dan ketentuan keselamatan dan keamanan. Pada Gambar 8.5 diperlihatkan bahwa BSSN memberikan rekomendasi, persyaratan, dan tolak ukur terkait keamanan komputer kepada BAPETEN. Selanjutnya, BAPETEN menjadikannya dasar dalam penyusunan panduan dan persyaratan peraturan di bidang keamanan komputer untuk membantu operator terkait implementasinya. BAPETEN harus memastikan bahwa setiap operator memiliki program keamanan komputer yang menjelaskan langkah-langkah keamanan komputernya. BAPETEN harus memverifikasi kepatuhan lanjutan dengan persyaratan peraturan dan kondisi lisensi yang berkaitan dengan keamanan komputer melalui inspeksi rutin. Selanjutnya, bila perlu, penggunaan tindakan penegakan untuk memastikan bahwa tindakan korektif tepat waktu dapat diambil.

Adapun peranan operator adalah mematuhi sertifikasi, tolak ukur, serta persyaratan peraturan yang ditetapkan oleh otoritas kompeten, baik BSSN maupun BAPETEN. Kemudian otoritas kompeten bersama operator menetapkan persyaratan kontrak pada vendor, kontraktor, dan pemasok untuk menerapkan langkah-langkah keamanan komputer yang sepadan dengan peran mereka (BEIS, 2022). Persyaratan kontrak harus merinci langkah-langkah keamanan komputer untuk memastikan bahwa aktivitas kedua belah pihak tidak menyediakan celah untuk serangan siber di pihak lain dan bahwa informasi sensitif kedua belah pihak dilindungi dengan tepat.

Otoritas kompeten dan operator juga secara berkala mengevaluasi langkah-langkah keamanan komputer untuk memastikan bahwa persyaratan peraturan dipatuhi. Kegiatan evaluasi dapat mencakup audit, tinjauan, pengujian kinerja, dan pelatihan yang sesuai. Evalusi juga perlu dilakukan ketika sistem berbasis komputer dimodifikasi, untuk mempertimbangkan apakah modifikasi tersebut dapat menimbulkan kerentanan baru dan/atau menciptakan aset digital sentitif baru. Periode evaluasi ditetapkan untuk memperhitungkan setiap perubahan ancaman, atau faktor lain yang memengaruhi risiko.

F. Penerapan Keamanan Informasi Nuklir di BATAN

Penerapan keamanan informasi secara umum di Badan Tenaga Nuklir Nasional (BATAN)—dapat dikatakan—dimulai dengan memanfaatkan momentum dari berbagai kejadian atau munculnya ketetapan baru atau proyek baru dari pemerintah atau instansi terkait, meskipun hal itu tidak langsung berkaitan dengan keamanan informasi. Sebagai contoh, dengan ditetapkannya Undang-undang Hak Cipta pada tahun 2002 yang menjadi salah satu penyebab dicetuskannya proyek *Indonesia Go Open Source* (IGOS) pada tahun 2004, BATAN menjawab dengan mulai mengkampanyekan penggunaan *software* legal dalam internal BATAN. Selain sebagai bukti kepatuhan pada peraturan yang berlaku, hal tersebut juga didorong oleh kesadaran akan adanya risiko keamanan dalam setiap penggunaan *software* bajakan.

Kemudian, masih dalam rangka menurunkan risiko keamanan yang sama, sejak tahun 2005, melalui penyelenggaraan *workshop* untuk internal, BATAN menjadi salah satu dari sedikit instansi pemerintah yang ikut mendorong penggunaan *software* legal dengan menawarkan aplikasi berbasis kode terbuka (*open source*) sebagai pilihan alternatif yang aman dari sisi keamanan informasi.

Ditetapkannya UU ITE pada tahun 2008 dan surat edaran dari Menteri Komunikasi dan Informatika Nomor: 05/SE/M.KOMINFO/07/2011 tentang Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, mendorong BATAN untuk memberi perhatian yang lebih besar pada keamanan data digital

yang dimiliki. Kampanye untuk meningkatkan kesadaran keamanan informasi dalam internal BATAN melalui *workshop* Keamanan Informasi (KAMI) yang diselenggarakan setiap tahun, mendapat *feedback* yang cukup bagus dari para peserta yang pernah mengikuti *workshop* tersebut. Hal yang perlu dicatat adalah kapasitas jumlah peserta *workshop* yang bisa ditampung setiap tahun, sama sekali tidak sebanding dengan penambahan pegawai BATAN. Di sisi lain, berbagai kejadian di dunia siber dan perkembangan baru di teknologi informasi menuntut pembaruan isi dan metode *workshop*. Hal ini membuat isi *workshop* beberapa tahun sebelumnya ketinggalan zaman.

Tidak hanya terbatas pada peningkatan kesadaran keamanan informasi, peningkatan dan penguatan kemampuan pelaku IT di BATAN juga dilaksanakan meskipun menghadapi berbagai keterbatasan. Dalam berbagai kesempatan, satu atau beberapa orang diikutsertakan pada kursus atau pelatihan, baik yang diselenggarakan oleh badan pemerintah maupun oleh swasta, baik untuk mendapatkan sertifikasi maupun yang tidak. Beberapa kesempatan keikutsertaan dalam *Regional Training Course* yang diselenggarakan oleh IAEA ataupun lembaga regulator tenaga nuklir dari negara lain juga dimanfaatkan untuk meningkatkan kemampuan sumber daya manusia (SDM) IT BATAN dalam mengelola keamanan informasi.

Sejak tahun 2018, BATAN juga menjalin kerja sama dengan United State-Department of Energy (US-DoE) dalam hal pelatihan keamanan informasi. Pelatihan yang diselenggarakan, selain diikuti oleh staf IT BATAN juga diikuti oleh beberapa peserta dari instansi lain, seperti BAPETEN dan BSSN.

Selain peningkatan kesadaran akan keamanan informasi dan peningkatan kemampuan SDM, BATAN juga menerapkan kontrol keamanan informasi yang lebih ketat. Kontrol teknis dan administratif dilakukan dalam penerapan topologi terpusat pada jaringan dalam dan antarkawasan BATAN. Pusat-pusat riset di BATAN tidak diperbolehkan untuk melanggan jaringan internet sendiri dan hanya boleh menggunakan jaringan BATAN yang terpusat. Meskipun terpusat, kontrol teknis yang diterapkan dalam topologi diatur sedemikian

rupa sehingga insiden keamanan informasi bisa dilokalisir dan tidak mengurangi atau mengganggu fungsionalitas jaringan dan server di tempat lain. Semua itu dilakukan dengan tetap mempertahankan *air gap* antara jaringan bisnis dan jaringan internal fasilitas nuklir. Kontrol administratif juga diterapkan, misalnya dalam pengelolaan hak akses pengguna pada sumber daya tertentu. Beberapa peraturan internal yang ditujukan untuk mendukung kontrol administratif diterbitkan, seperti surat edaran penggunaan email. Selain itu, peraturan internal termutakhir adalah ditetapkannya Peraturan BATAN Nomor 5 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di BATAN pada tanggal 5 Mei 2021, yang memasukkan unsur keamanan sebagai salah satu prinsip dasar pelaksanaannya.

Selain kontrol teknis dan administratif, kontrol fisik juga diterapkan melalui kerjasama dengan unit pengamanan kawasan nuklir, seperti dalam hal hak akses ke gedung atau ruangan simpul infrastruktur IT yang kritikal.

Sisi pengelolaan informasi pun tidak luput dari perhatian, dengan memaksimalkan sumber daya yang terbatas. BATAN telah memiliki sistem *backup* data yang cukup berguna untuk menjamin ketersediaan data, bila sistem penyimpanan utama mengalami gangguan. BATAN memanfaatkan beberapa perangkat *firewall* untuk memfilter data yang berpotensi merusak.

Dengan semakin menguatnya isu keamanan informasi di dalam negeri yang dipicu oleh peretasan terhadap beberapa situs penting di Indonesia, BATAN pun terpacu untuk segera membentuk tim tanggap darurat insiden siber. Melalui tahapan yang cukup panjang, yang dimulai pada 28 Agustus 2019, dilakukan asistensi pertama dengan BSSN terkait pembentukan BATAN-CSIRT (Computer Security Incident Reporting Team). Setelah asistensi pertama, kerja sama antara BATAN dan BSSN terus ditingkatkan. Hal ini ditandai pada saat diselenggarakannya pelatihan *Cyber Security for Nuclear & Radiological Facilities* (30 September–4 Oktober 2019), yang merupakan pelatihan kedua terkait keamanan informasi dengan bekerja sama dengan US-DoE. BATAN turut juga mengundang staf BSSN untuk hadir sebagai

peserta pada pelatihan tersebut. Bertepatan dengan ulang tahun BATAN tanggal 5 Desember 2019, MOU antara BATAN dan BSSN mengenai kerja sama terkait tanda tangan digital dan pembentukan CSIRT di BATAN, ditandatangani. Pada tahun 2021, Surat Keputusan (SK) Kepala Pusat Pendayagunaan Informatika dan Kawasan Nuklir (PPIKSN) tentang pembentukan Tim Cyber Security BATAN disahkan dan pada akhirnya pada tanggal 25 Mei 2021, BATAN-CSIRT resmi diluncurkan (Gambar 8.6).

Foto: Dokumentasi BATAN (2021)

Gambar 8.6 Peluncuran BATAN-CSIRT Bersama BSSN

Penerapan keamanan informasi nuklir di BATAN memang masih dititikberatkan pada sistem komputer dan jaringan bisnis BATAN. Selain karena berbagai data penting ketenaganukliran berlokasi di dalam jaringan tersebut, adanya *air gap* antara jaringan bisnis dan jaringan kontrol fasilitas nuklir turut menciptakan kontrol keamanan. Hal ini bersamaan dengan berbagai usaha peningkatan kesadaran keamanan informasi di internal BATAN, pelatihan sumber daya manusia, perbaikan dan penyederhanaan topologi jaringan, penerapan berbagai kontrol keamanan dan pengembangan sistem komputer

yang lebih mendukung ketersediaan data, dengan tetap menjamin kerahasiaan dan integritas data, dengan payung aturan dan hukum yang telah terbit.

G. Penutup

Ancaman serangan siber berkembang secara terus-menerus dengan frekuensi dan tingkat keparahan kejahatan penyusupan yang makin kompleks dan dengan kecepatan yang mengkhawatirkan. Perlindungan terhadap infrastruktur IT dan data milik lembaga pemerintahan akan menjadi tantangan yang selalu berkembang makin besar bagi setiap personel yang ditugaskan untuk menjaga infrastruktur tersebut. Hal ini menjadi tugas dan tanggungjawab kita untuk saling berbagi pengetahuan, membangun kerja sama privat dan publik, menerapkan aksi inisiatif baru, dan tetap waspada terhadap ancaman yang bisa mencelakakan kita.

Setelah BATAN dan Lembaga Pemerintah NonKemeterian riset lain serta badan penelitian dan pengembangan di berbagai kementerian berintegrasi ke dalam Badan Riset dan Inovasi Nasional (BRIN), kontrol keamanan informasi nuklir menjadi tantangan tersendiri. Hal ini mengingat luasnya ruang lingkup kerja BRIN, baik dari sisi domain riset maupun lokasi fisik sehingga sistem berbasis komputer menjadi basis dari banyak kegiatan. Di satu sisi, hal tersebut sebagai solusi efisiensi dan efektivitas kerja, tetapi di sisi lain juga membuka tantangan terhadap keamanan informasi yang sensitif, khususnya tentang aset digital sensitif yang terkait dengan bahan nuklir dan fasilitas nuklir.

Berdasarkan Prinsip *Fundamental L Ammendement of CPPNM*, negara diharuskan menetapkan persyaratan untuk kerahasiaan informasi, termasuk aset digital sensitif, yang terkait dengan bahan nuklir dan fasilitas nuklir. Dalam hal ini, dan dalam lingkup BRIN, kewajiban negara dapat dilakukan oleh BRIN sebagai badan pelaksana ketenaganukliran dan sebagai pemegang izin berbagai bahan nuklir dan fasilitas nuklir. Kriteria kerahasiaan informasi tersebut perlu didasarkan pada dampak dari terbukanya informasi secara tidak sah

yang akan berpengaruh terhadap pelemahan sistem proteksi fisik terhadap bahan nuklir dan fasilitas nuklir terkait.

Daftar Referensi

Alexander, R. D., & Panguluri, S. (2016). Cybersecurity terminology and frameworks. Dalam R. Clark, & S. Hakim (Ed.), *Cyber-Physical Security. Protecting Critical Infrastructure, vol 3.* Springer. https://link.springer.com/chapter/10.1007/978-3-319-32824-9_2#citeas

Anjani, N. H. (2021). *Ringkasan kebijakan no. 9: Perlindungan keamanan siber di Indonesia. Center for Indonesian Policy Studies*. https://www.cips-indonesia.org/publications/perlindungan-keamanan-siber-di-indonesia

Chryshna, M. (2021, 4 Juli). Badan Siber dan Sandi Negara (BSSN). *Kompaspedia*. https://kompaspedia.kompas.id/baca/profil/lembaga/badan-siber-dan-sandi-negara-bssn

Department for Business, Energy & Industrial Strategy. (2022). *2022 Civil Nuclear Cyber Security Strategy.* UK Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1075002/civil-nuclear-cyber-security-strategy-2022.pdf

International Atomic Energy Agency. (2011a). Nuclear security recommendations on physical protection of nuclear material and facilities (INFCIRC/225/Revision 5). *IAEA Nuclear Security Series No. 13.* https://www.iaea.org/publications/8629/nuclear-security-recommendations-on-physical-protection-of-nuclear-material-and-nuclear-facilities-infcirc225revision-5

International Atomic Energy Agency. (2011b). Nuclear security recommendations on radioactive material and associated facilities. *IAEA Nuclear Security Series No. 14*. https://www.iaea.org/publications/8616/nuclear-security-recommendations-on-radioactive-material-and-associated-facilities

International Atomic Energy Agency. (2011c). Nuclear security recommendations on nuclear and other radioactive material out of regulatory control. *IAEA Nuclear Security Series No 15.* https://www.iaea.org/publications/8622/nuclear-security-recommendations-on-nuclear-and-other-radioactive-material-out-of-regulatory-control

International Atomic Energy Agency. (2013). Objective and essential elements of a state's nuclear security regime. *IAEA Nuclear Security*

Series No. 20. https://www.iaea.org/publications/10353/objective-and-essential-elements-of-a-states-nuclear-security-regime
International Atomic Energy Agency. (2015). Security of Nuclear Information. *IAEA Nuclear Security Series No. 23-G.* https://www.iaea.org/publications/10774/security-of-nuclear-information
International Atomic Energy Agency. (2016). Amendment to the convention on the physical protection of nuclear material. *INFCIRC/274/Rev.1/Mod.1.*
International Atomic Energy Agency. (2021a). Computer security techniques for nuclear facilities. *IAEA Nuclear Security Series No. 17-T (Rev. 1).* https://www.iaea.org/publications/14729/computer-security-techniques-for-nuclear-facilities
International Atomic Energy Agency. (2021b, 1–12 November). *Information and computer security.* Regional School on Nuclear Security for Asia and the Pacific, Jakarta, Indonesia.
International Atomic Energy Agency. (2021c). Computer security for nuclear security. *IAEA Nuclear Security Series No. 42-G.* https://www.iaea.org/publications/13629/computer-security-for-nuclear-security
International Atomic Energy Agency. (2018). Computer Security of Instrumentation and Control Systems at Nuclear Facilities: Technical Guidance. *IAEA Nuclear Security Series No. 33-T*. https://www.iaea.org/publications/11184/computer-security-of-instrumentation-and-control-systems-at-nuclear-facilities
Kim, S., Heo, G., Zio, E., Shin, J., & Song, J. (2020). Cyber attack taxonomy for digital environment in nuclear power plants. *Nuclear Engineering and Technology, 52(*5), 995–1001. https://doi.org/10.1016/j.net.2019.11.001
Park, J., Suh, Y. (2014). A development framework for software security in nuclear safety system: Integrating secure development and system security activities. *Nuclear Engineering and Technology, 46*(1), 47–54. https://doi.org/10.5516/NET.04.2012.061
Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 tentang Pedoman Pertahanan Siber. (2014). https://peraturan.bpk.go.id/Details/177738/permenhan-no-82-tahun-2014
Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital. (2022). https://peraturan.bpk.go.id/Details/211029/perpres-no-82-tahun-2022
Setiyawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). upaya regulasi teknologi informasi dalam menghadapi serangan siber (*cyber attack*)

guna menjaga kedaulatan Negara Kesatuan Republik Indonesia. *Jurnal USM Law Review, 3*(2), 275–295. https://journals.usm.ac.id/index.php/julr/article/view/2773

Shalal, A. (2016, 10 Oktober). IAEA chief: Nuclear power plant was disrupted by cyber attack. *Reuters.* https://www.reuters.com/article/us-nuclear-cyber-idUSKCN12A1OC

Undang-undang Republik Indonesia No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). https://peraturan.bpk.go.id/Details/37589/uu-no-11-tahun-2008

Undang-undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2016). https://peraturan.bpk.go.id/Details/37582/uu-no-19-tahun-2016