RSNI3

Rancangan Standar Nasional Indonesia 3

RSNI3 ISO/IEC 27032:2023
(Ditetapkan oleh BSN tahun 2024)

Keamanan siber – Pedoman untuk keamanan Internet

Cybersecurity — Guidelines for Internet security

(ISO/IEC 27032:2023, IDT)

Pengguna dari RSNI ini diminta untuk menginformasikan adanya hak paten dalam dokumen ini, bila diketahui, serta memberikan informasi pendukung lainnya (pemilik paten, bagian yang terkena paten, alamat pemberi paten dan lain-lain)

ICS 35.030

BADAN STANDARDISASI NASIONAL

BSN
Email: dokinfo@bsn.go.id
www.bsn.go.id

Diterbitkan di Jakarta

Daftar isi

Daftar isi i
Prakata iii
Pendahuluan iv
1 Ruang lingkup 1
2 Acuan normatif 1
3 Istilah dan definisi 1
4 Istilah singkatan 5
5 Hubungan antara keamanan Internet, keamanan web, keamanan jaringan, dan keamanan siber 6
6 Gambaran umum keamanan Internet 7
7 Pihak yang berkepentingan 9
7.1 Umum 9
7.2 Pengguna 9
7.3 Koordinator dan organisasi standardisasi 10
7.4 Otoritas pemerintah 11
7.5 Lembaga penegak hukum 11
7.6 Penyedia layanan Internet 11
8 Asesmen dan penanganan risiko keamanan Internet 12
8.1 Umum 12
8.2 Ancaman 12
8.3 Kerentanan 13
8.4 Vektor serangan 14
9 Pedoman keamanan Internet 15
9.1 Umum 15
9.2 Kontrol keamanan Internet 16
9.2.1 Umum 16
9.2.2 Kebijakan keamanan Internet 16
9.2.3 Kontrol akses 16
9.2.4 Edukasi, kesadaran, dan pelatihan 17
9.2.5 Manajemen insiden keamanan 18
9.2.6 Manajemen aset 19
9.2.7 Manajemen pemasok 20
9.2.8 Keberlangsungan bisnis melalui Internet 21
9.2.9 Proteksi privasi melalui Internet 21
9.2.10 Manajemen kerentanan 22

9.2.11 Manajemen jaringan 23
9.2.12 Proteksi terhadap perangkat perusak 24
9.2.13 Manajemen perubahan 25
9.2.14 Identifikasi undang-undang yang berlaku dan persyaratan kepatuhan 25
9.2.15 Penggunaan kriptografi 25
9.2.16 Keamanan aplikasi untuk aplikasi hadap-Internet 26
9.2.17 Manajemen perangkat titik akhir 27
9.2.18 Pemonitoran 28
Lampiran A (informatif) Rujukan silang antara dokumen ini dan ISO/IEC 27002 29
Bibliografi 31

Prakata

Standar Nasional Indonesia (SNI) ISO/IEC 27032:2023 dengan judul Keamanan siber – Pedoman untuk keamanan Internet merupakan standar revisi dari SNI ISO/IEC 27032:2014 dengan judul Teknologi informasi - Teknik keamanan - Pedoman keamanan siber. Standar ini disusun dengan jalur adopsi identik dari ISO/IEC 27032:2023 dengan judul Cybersecurity – Guidelines for internet security, dengan metode adopsi terjemahan dua bahasa dan ditetapkan oleh BSN Tahun 2024.

Standar ini menggantikan SNI ISO/IEC 27032:2024 dengan judul Teknologi informasi – Teknik keamanan – Pedoman keamanan siber, yang disusun dengan metode adopsi *republication-reprint* dan ditetapkan oleh BSN Tahun 2024.

Standar ini disusun oleh Komite Teknis 35-04, Keamanan Informasi, Keamanan Siber dan Perlindungan Privasi. Standar ini telah dibahas dan disetujui dalam rapat konsensus nasional di Depok pada tanggal 21 Juni 2024. Konsensus ini dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari produsen, konsumen, pakar dan pemerintah. Standar ini telah melalui tahap jajak pendapat pada tanggal 18 Juli 2024 sampai dengan 1 Agustus 2024 dengan hasil akhir disetujui menjadi SNI.

Terdapat standar ISO/IEC yang digunakan sebagai acuan dalam standar ini telah diadopsi menjadi Standar Nasional Indonesia (SNI) sebagai berikut:

– ISO/IEC 27000, *Information technology — Security techniques — Information security management systems – Overview and vocabulary* telah diadopsi secara identik menjadi SNI ISO/IEC 27000:2018, Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Gambaran umum dan kosakata

Perlu diperhatikan bahwa kemungkinan beberapa unsur dari standar ini dapat berupa hak kekayaan intelektual (HAKI). Namun selama proses perumusan SNI, Badan Standardisasi Nasional telah memperhatikan penyelesaian terhadap kemungkinan adanya HAKI terkait substansi SNI. Apabila setelah penetapan SNI masih terdapat permasalahan terkait HAKI, Badan Standardisasi Nasional tidak bertanggung jawab mengenai bukti, validitas, dan ruang lingkup dari HAKI tersebut.

Apabila pengguna menemukan keraguan dalam standar ini maka disarankan untuk melihat standar aslinya, yaitu ISO/IEC 27032:2023 (E) dan/atau dokumen terkait lain yang menyertainya.

Pendahuluan

Fokus dari dokumen ini adalah untuk mengatasi masalah keamanan Internet dan memberikan panduan untuk mengatasi ancaman keamanan Internet yang umum, seperti:
— serangan rekayasa sosial;
— serangan *zero-day*;
— serangan privasi;
— peretasan; dan
— proliferasi perangkat perusak (*malware*), perangkat pengintai, dan perangkat lunak berpotensi tak dikehendaki lainnya.

Panduan dalam dokumen ini memberikan kontrol teknis dan nonteknis untuk mengatasi risiko keamanan Internet, termasuk kontrol untuk:
— mempersiapkan menghadapi serangan;
— mencegah serangan;
— mendeteksi dan memonitor serangan; dan
— merespons serangan.

Panduan ini berfokus pada penyediaan praktik terbaik industri, edukasi konsumen dan pegawai secara luas untuk membantu pihak yang berkepentingan dalam memainkan peran aktif untuk mengatasi tantangan keamanan Internet. Dokumen ini juga berfokus pada pelindungan konfidensialitas, integritas, dan availabilitas informasi melalui Internet dan properti lainnya, seperti autentisitas, akuntabilitas, nonrepudiasi, dan reliabilitas yang juga dapat dilibatkan.

Hal ini termasuk panduan keamanan Internet untuk:
— peranan;
— kebijakan;
— metode;
— proses; dan
— kontrol teknis yang aplikabel.

Berdasarkan cakupan dokumen ini, kontrol yang diberikan diharuskan berada pada level tinggi. Standar dan pedoman spesifikasi teknis mendetail yang aplikabel untuk setiap area dirujuk dalam dokumen ini untuk panduan lebih lanjut. Lihat Lampiran A untuk korespondensi di antara kontrol yang dikutip dalam dokumen ini dan kontrol dalam ISO/IEC 27002.

Dokumen ini tidak secara spesifik membahas kontrol yang dapat disyaratkan organisasi untuk sistem yang mendukung infrastruktur kritikal atau keamanan nasional. Namun, sebagian besar kontrol yang disebutkan dalam dokumen ini dapat diaplikasikan pada sistem tersebut.

Dokumen ini menggunakan konsep yang sudah ada dari ISO/IEC 27002, seri ISO/IEC 27033, ISO/IEC TS 27100 dan ISO/IEC 27701, untuk mengilustrasikan:
— hubungan antara keamanan Internet, keamanan web, keamanan jaringan, dan keamanan siber;
— panduan mendetail tentang kontrol keamanan Internet yang dikutip dalam 9.2, yang membahas kesiapan keamanan-siber untuk sistem yang hadap-Internet (*Internet-facing*).

Seperti yang disebutkan dalam ISO/IEC TS 27100, Internet adalah jaringan global, yang digunakan oleh organisasi untuk semua komunikasi, baik digital dan suara. Berdasarkan beberapa pengguna menargetkan serangan terhadap jaringan ini, maka kritikal untuk mengatasi risiko keamanan yang relevan.

Keamanan siber – Pedoman untuk keamanan Internet

1 Ruang lingkup

Dokumen ini memberikan:

— penjelasan hubungan antara keamanan Internet, keamanan web, keamanan jaringan, dan keamanan siber;

— gambaran umum keamanan Internet;

— identifikasi pihak yang berkepentingan dan deskripsi peranannya dalam keamanan Internet;

— panduan tingkat tinggi untuk mengatasi masalah keamanan Internet yang umum.

Dokumen ini dimaksudkan untuk organisasi yang menggunakan Internet.

2 Acuan normatif

Dokumen berikut dirujuk dalam teks sedemikian rupa sehingga sebagian atau seluruh isinya mendasari persyaratan dokumen ini. Untuk rujukan bertanggal, hanya edisi yang dikutip yang berlaku. Untuk rujukan yang tidak bertanggal, berlaku edisi terakhir dari dokumen yang dirujuk (termasuk setiap amandemennya).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Istilah dan definisi

Untuk tujuan dokumen ini, berlaku istilah dan definisi berikut dan yang diberikan dalam ISO/IEC 27000.

ISO and IEC memelihara basis data terminologi untuk digunakan dalam standardisasi di alamat berikut:

— Platform penelusuran ISO daring: tersedia di https://www.iso.org/obp

— IEC Electropedia: tersedia di http://www.electropedia.org/

3.1
vektor serangan
jalur atau cara yang digunakan oleh penyerang untuk dapat memperoleh akses ke komputer atau server jaringan sehingga memberikan manfaat yang merusak.

CONTOH 1 perangkat IoT.

CONTOH 2 ponsel pintar.

3.2
penyerang
orang yang dengan sengaja mengeksploitasi kerentanan dalam kontrol keamanan teknis dan nonteknis untuk mencuri atau membobol sistem dan jaringan informasi, atau untuk membobol availabilitas sumber daya sistem dan jaringan informasi bagi pengguna yang sah

[SUMBER: ISO/IEC 27033-1:2015, 3.3]

3.3
serangan bauran
serangan yang berupaya untuk memaksimalkan keparahan kerusakan dan kecepatan penularan dengan mengombinasikan berbagai *vektor serangan* (3.1)

3.4
bot
program perangkat lunak terautomasi yang digunakan untuk melakukan tugas yang spesifik

Catatan 1 untuk entri: Kata ini sering digunakan untuk mendeskripsikan program, yang biasanya dijalankan di server, yang mengotomatisasi tugas seperti meneruskan atau menyortir surel.

Catatan 2 untuk entri: Bot juga dideskripsikan sebagai program yang beroperasi sebagai agen untuk pengguna atau program lain atau menyimulasikan aktivitas manusia. Pada Internet, bot yang paling banyak ditemui adalah program, yang juga disebut *spiders* atau *crawlers*, yang mengakses situs web dan mengumpulkan isinya untuk indeks mesin pencari.

3.5
botnet
kumpulan bot perusak yang dikontrol dari jarak jauh yang berjalan secara mandiri atau otomatis pada komputer yang terbobol

CONTOH: Simpul kegagalan layanan secara terdistribusi (*Distributed denial-of-service* (DDoS)), di mana pengontrol *botnet* dapat memerintah komputer pengguna untuk menghasilkan trafik ke situs pihak ketiga sebagai bagian dari serangan DDoS terkoordinasi.

3.6
keamanan siber
pelindungan orang, masyarakat, organisasi, dan negara dari risiko siber

Catatan 1 untuk entri: Pelindungan berarti menjaga risiko siber pada level yang dapat ditoleransi.

[SUMBER: ISO/IEC TS 27100:2020, 3.2]

3.7
***dark net* (jaringan gelap)**
jaringan situs web rahasia di Internet yang hanya dapat diakses dengan perangkat lunak spesifik

Catatan 1 untuk entri: *Dark net* juga dikenal sebagai *dark web*.

3.8
perangkat lunak yang menipu (*deceptive software*)
perangkat lunak yang melakukan aktivitas di komputer pengguna tanpa terlebih dahulu memberi tahu pengguna tentang apa sebenarnya yang akan dilakukan perangkat lunak tersebut di komputer, atau meminta persetujuan pengguna atas tindakan tersebut

CONTOH 1 Program yang membajak konfigurasi pengguna.

CONTOH 2 Program yang menyebabkan iklan muncul terus menerus yang tidak dapat dihentikan dengan mudah oleh pengguna.

CONTOH 3 Perangkat lunak beriklan dan perangkat pengintai.

3.9
peretasan
secara sengaja mengakses sistem komputer tanpa otorisasi pengguna atau pemiliknya

3.10
hacktivism
peretasan (3.9) untuk tujuan bermotif politik atau sosial

3.11
Internet
sistem global dari jaringan yang terinter-koneksi dalam domain publik

[SUMBER: ISO/IEC 27033-1:2015, 3.14, dimodifikasi — "*the*" telah dihapus dari istilah.]

3.12
keamanan Internet
preservasi konfidensialitas, integritas, dan ketersediaan informasi melalui *Internet* (3.11)

Catatan 1 untuk entri: Sebagai tambahan, properti lain seperti autentisitas, nonrepudiasi, dan reliabilitas juga dapat dilibatkan.

Catatan 2 untuk entri: Silakan merujuk pada definisi konfidensialitas, integritas, ketersediaan, autentisitas, akuntabilitas, nonrepudiasi, dan reliabilitas dalam ISO/IEC 27000:2018, Pasal 3.

3.13
penyedia layanan Internet *(Internet service provider)*
ISP
organisasi yang menyediakan layanan Internet kepada pengguna dan memungkinkan pelanggannya untuk mengakses *Internet* (3.11)

Catatan 1 untuk entri: Juga terkadang disebut sebagai penyedia akses Internet (*Internet access provider*-IAP).

3.14
konten yang merusak
aplikasi, dokumen, fail, data, atau sumber daya lainnya yang dapat memiliki fitur atau kapabilitas yang merusak yang tertanam, tersamar, atau tersembunyi di dalamnya

3.15
perangkat perusak
malicious software
perangkat lunak yang didesain dengan maksud jahat yang berisi fitur atau kapabilitas yang dapat berpotensi menyebabkan kerugian secara langsung atau tidak langsung terhadap pengguna dan/atau sistem komputer pengguna

CONTOH Virus, *worm*, dan *trojan*.

3.16
organisasi
orang atau sekelompok orang yang memiliki fungsi sendiri dengan tanggung jawab, otoritas, dan hubungan untuk mencapai tujuannya.

Catatan 1 untuk entri: Dalam konteks dokumen ini, individu berbeda dengan organisasi.

Catatan 2 untuk entri: Secara umum, pemerintah juga merupakan sebuah organisasi. Dalam konteks dokumen ini, pemerintah dapat dipertimbangkan terpisah dari organisasi lain demi kejelasan.

[SUMBER: ISO 9000:2015, 3.2.1, dimodifikasi — Catatan 1 untuk entri dan Catatan 2 untuk entri telah diganti.]

3.17
***phishing* (pengelabuan)**
proses penipuan yang berupaya memperoleh informasi pribadi atau konfidensial dengan menyamar sebagai entitas yang terpercaya dalam komunikasi elektronik

Catatan 1 untuk entri: *Phising* dapat dicapai dengan menggunakan rekayasa sosial atau penipuan teknis.

3.18
perangkat lunak berpotensi tak dikehendaki
perangkat lunak yang menipu (3.8), termasuk *perangkat perusak* (3.15) dan tak perusak, yang menunjukkan karakteristik perangkat lunak yang menipu

3.19
spam
surel yang tidak diharapkan yang dapat membawa konten yang merusak dan/atau pesan tipuan

Catatan 1 untuk entri: Meskipun bentuk yang paling dikenal luas dari spam adalah spam surel, istilah ini diterapkan pada penyalahgunaan serupa di media lain: spam pesan instan, spam grup berita Usenet, spam mesin pencari Web, spam di blog, spam wiki, spam pesan ponsel, spam forum Internet, dan transmisi faks sampah.

[SUMBER: ISO/IEC 27033-1:2015, 3.37, dimodifikasi — Catatan 1 untuk entri telah ditambahkan.]

3.20
perangkat pengintai
perangkat lunak yang menipu (3.8), yang mengumpulkan informasi pribadi atau konfidensial dari pengguna komputer

Catatan 1 untuk entri: Informasi dapat termasuk hal-hal seperti situs web yang paling sering dikunjungi atau informasi yang lebih sensitif seperti kata sandi.

3.21
ancaman
penyebab potensial dari insiden yang tidak diinginkan, yang dapat menyebabkan kerugian pada sistem, individu, atau *organisasi* (3.16)

3.22
trojan
perangkat perusak (3.15) yang tampaknya melakukan fungsi yang diinginkan pengguna tetapi yang menyesatkan pengguna tentang maksud sebenarnya

3.23
vishing
pengelabuan suara (*voice phishing*) yang dilakukan untuk memperoleh informasi pribadi atau konfidensial dengan menyamar sebagai entitas yang tepercaya

Catatan 1 untuk entri: *Vishing* dapat dilakukan melalui surel suara, VoIP (suara melalui IP), atau telepon rumah atau ponsel.

3.24
teknik *waterhole* (lubang air)
teknik yang menghasut orang untuk mengakses situs web yang secara spesifik berisi (banyak) perangkat perusak

Catatan 1 untuk entri: *Waterhole* juga dikenal sebagai *watering hole*.

3.25
World Wide Web
Web
dunia informasi dan layanan yang dapat diakses melalui jaringan

[SUMBER: ISO 19101-1:2014, 4.1.40]

4 Istilah singkatan

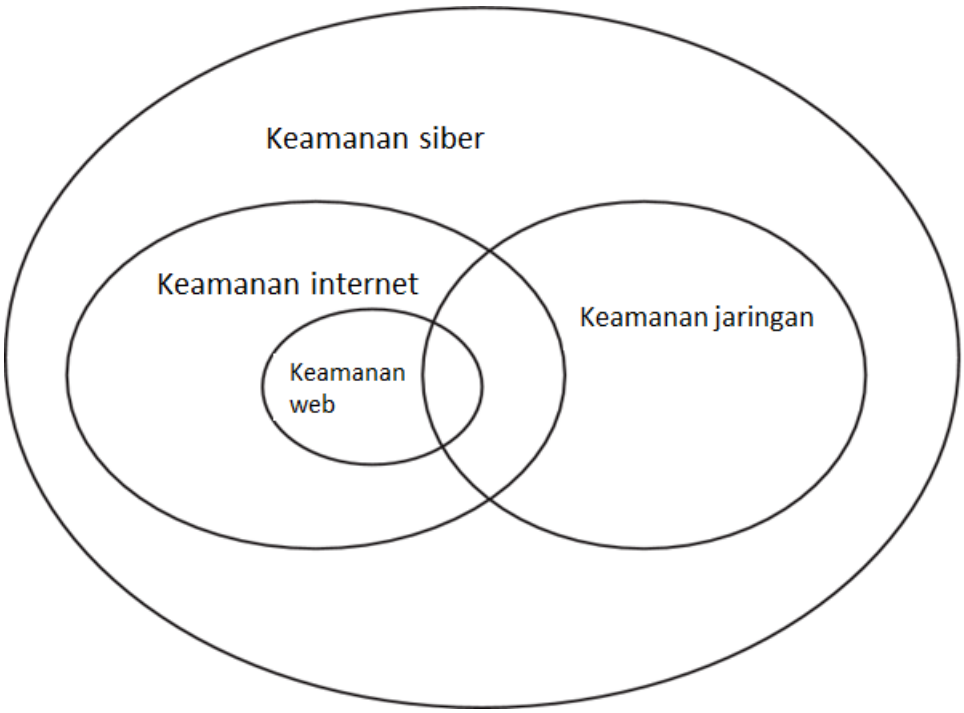
Istilah singkatan berikut digunakan dalam dokumen ini.

KA	kecerdasan artifisial (*artificial intelligence*)
API	antarmuka pemrograman aplikasi (*application programming interface*)
APT	ancaman persisten tingkat lanjut (*advanced persistent threat*)
BYOD	bawa perangkat anda sendiri (*bring your own device*)
CERT	tim tanggap darurat komputer (*computer emergency response team*)
DDoS	serangan terdistribusi yang berakibat kegagalan layanan (*distributed denial-of-service*)
DLP	pencegahan kehilangan data (*data loss prevention*)
DMZ	zona demiliterisasi (*demilitarized zone*)
DNS	sistem nama domain (*domain name system*)
DoS	kegagalan layanan (*denial-of-service*)
EDR	deteksi dan respons titik akhir (*endpoint detection and response*)
FTP	protokol transfer fail (*file transfer protocol*)
HTTP	protokol transfer hiperteks (*hypertext transfer protocol*)
HTTPS	protokol transfer hiperteks melalui lapisan soket aman (*hypertext transfer protocol over secure socket layer*)
ICANN	korporasi Internet untuk nama dan nomor yang ditetapkan (*Internet corporation for assigned names and numbers*)
TIK	teknologi informasi dan komunikasi (*information and communications technology*)
IDS	sistem deteksi intrusi (*intrusion detection system*)
IETF	gugus tugas rekayasa Internet (*Internet engineering task force*)
IMT	tim manajemen insiden (*incident management team*)
IoT	Internet untuk segala (*Internet of things*)
IP	protokol Internet (*Internet protocol*)
IPS	sistem pencegahan intrusi (*intrusion prevention system*)
ISP	penyedia layanan Internet (*Internet service provider*)
ISV	vendor perangkat lunak independen (*independent software vendor*)
IRT	tim tanggap insiden (*incident response team*)

ISMS	sistem manajemen keamanan informasi *(information security management system*)
OWASP	proyek keamanan aplikasi web terbuka (*open web application security project*)
PII	informasi identifikasi pribadi (*personally identifiable information*)
SDLC	siklus hidup pengembangan perangkat lunak (*software development life cycle*)
SIEM	informasi keamanan dan manajemen kejadian (*security information and event management*)
SME	usaha kecil dan menengah (*small and medium enterprises*)
URL	lokator sumber daya uniform (*uniform resource locator*)
USB	perangkat seri universal (*universal serial bus*)
VPN	jaringan pribadi virtual (*virtual private network*)
W3C	konsorsium web seluruh dunia (*World Wide Web consortium*)
WWW	web seluruh dunia (*World Wide Web*)

5 Hubungan antara keamanan Internet, keamanan web, keamanan jaringan, dan keamanan siber

Gambar 1 menunjukkan pandangan tingkat tinggi mengenai hubungan antara keamanan Internet, keamanan web, keamanan jaringan, dan keamanan siber.



Gambar 1 — Hubungan antara keamanan Internet, keamanan web, keamanan jaringan, dan keamanan siber

Internet adalah sistem global dari jaringan digital yang terinter-koneksi dalam domain publik. Pertukaran informasi di Internet juga menggunakan jaringan telepon seluler yang kemudian menjadi bagian dari Internet. Jaringan global ini menghubungkan miliaran server, komputer, dan perangkat keras lainnya. Setiap perangkat terhubung dengan perangkat lain melalui koneksinya ke Internet. Internet menciptakan lingkungan yang kondusif untuk berbagi informasi.

Keamanan Internet berkaitan dengan memproteksi layanan hadap-Internet serta sistem dan jaringan TIK terkait sebagai perpanjangan dari keamanan jaringan. Upaya ini bertujuan untuk mengurangi risiko keamanan yang berhubungan dengan Internet bagi organisasi, pelanggan, dan pemangku kepentingan relevan lainnya.

Keamanan Internet juga memastikan ketersediaan dan reliabilitas layanan Internet. Melalui Internet, berbagai layanan ditawarkan, seperti layanan transfer fail, layanan surel, atau layanan lainnya yang dapat dibagikan secara publik kepada pengguna akhir. Dalam konteks ini, keamanan Internet berurusan dengan penyampaian layanan tersebut secara aman melalui jaringan publik.

Web adalah salah satu cara informasi dibagikan di Internet [yang lainnya termasuk surel, protokol transfer fail (*file transfer protocol*-FTP), dan layanan pesan instan]. Web tersusun dari miliaran dokumen digital yang terhubung dan dapat dilihat menggunakan peramban web. Situs web adalah serangkaian halaman web terkait yang disiapkan dan dipelihara sebagai kumpulan untuk mendukung satu tujuan.

Keamanan web berurusan dengan keamanan informasi dalam konteks *World Wide Web* (WWW) dan dengan layanan web yang diakses melalui jaringan publik. Layanan web diaktifkan dengan menggunakan protokol HTTP di mana setiap URL terdaftar yang tersedia secara publik dapat diakses. Keamanan web juga berurusan dengan keamanan koneksi HTTP ini yang digunakan untuk pertukaran informasi.

Jaringan dapat termasuk komponen seperti perute (*router*), hub, pengabelan, pengontrol telekomunikasi, pusat distribusi utama, dan perangkat kontrol teknis. Keamanan jaringan secara luas mencakup segala jenis jaringan yang ada dalam suatu organisasi mulai dari jaringan area lokal, jaringan area luas, jaringan area personal, dan jaringan nirkabel.

Keamanan jaringan berkaitan dengan desain, implementasi, pengoperasian dan peningkatan jaringan, serta identifikasi dan penanganan risiko keamanan yang berhubungan dengan jaringan dalam organisasi, antar-organisasi, dan antara organisasi dengan pengguna.

Keamanan siber berkaitan dengan mengelola risiko keamanan informasi ketika informasi berada dalam bentuk digital di komputer, penyimpanan, dan jaringan. Banyak kontrol, metode, dan teknik keamanan informasi yang dapat diterapkan untuk mengelola risiko siber.

Keamanan siber juga berurusan dengan memproteksi sistem yang terhubung-Internet termasuk perangkat keras, perangkat lunak, program, dan data dari potensi serangan. Banyak dari serangan ini dikarakterisasi oleh serangan bertarget dan bauran dengan tingkat kecanggihan dan persistensi yang tinggi. Ancaman dapat berupa berbasis-Internet dan/atau ancaman karena konektivitas dengan jaringan dan sistem lain dalam organisasi atau jaringan pelanggan dan penyedia layanan, yang menjadi tempat organisasi berkomunikasi selama kegiatan bisnis normal.

6 Gambaran umum keamanan Internet

Informasi pengidentifikasi personal (*personally identifiable information*–PII) pengguna Internet ditangkap oleh banyak situs dan layanan yang ditawarkan di Internet. Hal ini termasuk penyedia layanan aplikasi yang memantau dengan cermat aktivitas pengguna dan menggunakan teknik kecerdasan artifisial (KA) untuk memberikan rekomendasi pembelian, layanan kesehatan, manajemen waktu, dan sejumlah umpan balik lainnya yang bertujuan untuk membuat kehidupan dan tugas mereka lebih mudah dikelola. Banyak dari situs ini yang mengumpulkan data tersebut tanpa izin pengguna dan memberikan data kepada pihak ketiga lainnya untuk mendapatkan keuntungan moneter, sekali lagi tanpa sepengetahuan pengguna.

Pihak yang berkepentingan telah membangun kehadiran mereka di Internet melalui situs web, melakukan perdagangan elektronik dalam skala global, menyediakan layanan digital di Internet, menggunakan layanan *cloud* publik untuk menyampaikan layanan serta menggunakan aplikasi dan layanan bisnis berbasis web.

Banyak penggunaan Internet yang melibatkan pertukaran informasi dan penyediaan layanan yang tidak menyangkut masyarakat dan PII. PII bervariasi berdasarkan yurisdiksi. Keamanan informasi dan layanan semacam itu dapat menjadi kritikal bagi pihak yang berkepentingan. Selain itu, jangkauan perangkat keras yang terhubung ke Internet baik sebagai perangkat individual atau jaringan pribadi meningkat pesat dalam apa yang disebut Internet untuk segala. Otonomi dan penerapan kecerdasan artifisial dalam Internet menciptakan persyaratan keamanan Internet yang penuh tantangan.

Meskipun Internet dapat memfasilitasi manfaat bisnis yang signifikan, selalu ada banyak risiko keamanan untuk dimanajemeni. Penting untuk diingat bahwa Internet pada awalnya tidak didesain dengan mempertimbangkan fitur keamanan. Organisasi sangat bergantung pada penggunaan Internet untuk menjalankan bisnis mereka. Karena rendahnya tingkat kepercayaan yang berkaitan dengan Internet, operasi bisnis dapat menghadapi konsekuensi merugikan yang signifikan akibat hilangnya konfidensialitas, integritas, dan ketersediaan informasi dan layanan, jika tidak dikontrol secara memadai.

Sementara beberapa orang berhati-hati dalam mengelola identitas daring mereka, kebanyakan orang mengunggah detail profil pribadi mereka untuk dibagikan kepada orang lain. Profil di banyak situs, khususnya situs jejaring sosial dan ruang obrolan, dapat diunduh dan disimpan oleh pihak lain. Hal ini dapat mengakibatkan terciptanya berkas digital data pribadi yang dapat disalahgunakan, diungkapkan kepada pihak lain, atau digunakan untuk pengumpulan data sekunder. Walaupun akurasi dan integritas data ini dipertanyakan, data tersebut menciptakan kaitan dengan individu dan organisasi yang sering kali tidak dapat dihapus sepenuhnya. Perkembangan dalam bidang komunikasi, hiburan, transportasi, belanja, finansial, asuransi, dan layanan kesehatan ini menciptakan risiko baru bagi pihak yang berkepentingan di Internet. Oleh karena itu, risiko dapat dikaitkan dengan hilangnya privasi melalui Internet.

Konvergensi teknologi informasi dan komunikasi, kemudahan mengakses Internet dari komputer meja, laptop, hingga perangkat seluler dan IoT, serta menyempitnya ruang pribadi antar-individu, menarik perhatian pelaku kejahatan dan organisasi kriminal.

Entitas ini menggunakan mekanisme seperti *phishing*, spam, dan perangkat pengintai, serta mengembangkan teknik serangan seperti serangan *zero-day*, *vishing*, situs web yang merusak, dan teknik penipuan lainnya untuk mengeksploitasi kelemahan yang mereka temukan di Internet.

Dalam beberapa tahun terakhir, serangan keamanan di Internet telah berevolusi dari peretasan untuk ketenaran pribadi menjadi kejahatan terorganisasi atau kejahatan siber. Sejumlah besar alat dan proses yang sebelumnya diamati dalam insiden keamanan siber yang terisolasi, kini digunakan bersama-sama dalam serangan multi-bauran, yang sering kali memiliki tujuan merusak yang jauh jangkauannya.

Banyak dari alat ini juga tersedia di repositori perangkat lunak publik dan sumber daya lain yang tersedia secara publik. Tujuan serangan berkisar dari serangan personal, pencurian identitas, penipuan atau pencurian finansial, hingga *hacktivism* dan manipulasi informasi di Internet. Sebagian besar data pribadi dan data pelanggan yang dicuri juga dibuat tersedia di *dark net*, yang dapat diakses oleh publik. Organisasi, dan khususnya UKM, sebaiknya memahami konsekuensi nyata dari “manipulasi” informasi di Internet. Risiko keamanan ini adalah risiko siber bagi pengguna yang mengakses Internet.

Karena Internet adalah jaringan publik global, transaksi dapat berasal dari belahan dunia mana saja, begitu pula serangan. Berbagai modus transaksi bisnis yang dilakukan di Internet menjadi sasaran sindikat kejahatan siber. Mulai dari layanan bisnis-ke-bisnis, bisnis-ke-konsumen, hingga konsumen-ke konsumen, risiko yang ditimbulkan secara inheren kompleks.

Kompleksitas lain muncul dari fakta bahwa semua pihak yang berkepentingan, meskipun mereka tidak jahat, memiliki pandangan berbeda mengenai kebutuhan, persyaratan, dan ancaman mereka, sehingga mereka memiliki daftar risiko dan kontrol yang berbeda untuk menghadapinya. Artinya, tidak ada solusi yang “satu ukuran cocok untuk semua”.

Kriteria seperti hal yang mendasari transaksi atau perjanjian bergantung pada lingkungan hukum dan regulasi yang spesifik di seluruh yurisdiksi. Kriteria ini juga bergantung pada interpretasi hukum dan cara masing-masing pihak dalam hubungan tersebut mengelola tanggung jawabnya. Sering kali, permasalahan penggunaan data yang dikumpulkan selama transaksi atau hubungan tidak ditangani secara memadai. Hal ini pada akhirnya dapat menimbulkan masalah keamanan seperti kebocoran informasi.

Tantangan legal dan teknis yang ditimbulkan oleh permasalahan Internet ini mempunyai jangkauan yang luas dan bersifat global. Tantangan-tantangan ini hanya dapat diatasi melalui kolaborasi antara komunitas teknis keamanan informasi, komunitas legal, dan berbagai wilayah untuk mengadopsi strategi yang koheren. Strategi ini sebaiknya mempertimbangkan peran masing-masing pihak yang berkepentingan dan inisiatif yang ada, dalam kerangka kerja kooperasi internasional.

Informasi menyebar melalui Internet secara instan, artinya serangan juga dapat terjadi secara instan. Karena kecepatan ini tidak mudah dipahami oleh pikiran manusia, serangan selalu diketahui lama setelah hal itu terjadi, dan potensi kerusakan sudah sangat besar. Dalam kebanyakan kasus, identitas penyerang disembunyikan. Oleh karena itu, penggunaan kecerdasan artifisial (AI) sering diusulkan untuk melawan serangan tersebut.

7 Pihak yang berkepentingan

7.1 Umum

Pihak yang berkepentingan pada keamanan Internet termasuk pihak yang:
— menggunakan layanan melalui Internet;
— menggunakan Internet untuk menyediakan layanan;
— menyediakan infrastruktur dan kapabilitas komunikasi Internet;
— secara global mengoordinasikan pengoperasian Internet;
— menyediakan dan menegakkan hukum dan regulasi.

Pihak yang berkepentingan dengan keamanan Internet dapat dikategorikan sebagai pengguna (7.2), koordinator dan organisasi standardisasi (7.3), otoritas pemerintah (7.4), lembaga penegak hukum (7.5), dan penyedia layanan Internet (7.6).

7.2 Pengguna

Pengguna adalah istilah yang merujuk pada individu, pengguna akhir serta organisasi swasta dan publik yang menggunakan Internet. Organisasi swasta termasuk usaha kecil dan menengah (UKM), serta perusahaan besar. Pemerintah dan badan publik lainnya secara bersama-sama disebut sebagai organisasi publik. Seorang individu atau sebuah organisasi menjadi pengguna ketika mereka mengakses Internet atau setiap layanan yang tersedia melalui Internet. Pengguna dapat menggunakan layanan Internet, melihat, atau mengumpulkan informasi. Mereka juga dapat memberikan informasi spesifik tertentu yang

berada dalam ruang aplikasi, atau terbuka untuk anggota atau kelompok terbatas dalam ruang aplikasi, atau publik umum.

Peran pengguna dapat termasuk, tetapi tidak terbatas pada hal berikut:
— pengguna aplikasi Internet umum, atau pengguna umum, seperti pemain permainan daring, pengguna pesan instan, atau penjelajah web;
— pembeli/penjual, yang terlibat dalam penempatan barang dan layanan pada situs lelang dan pasar daring untuk pembeli yang berminat, dan sebaliknya;
— blogger dan kontributor konten lainnya (misalnya, penulis artikel di *wiki*), di mana informasi dalam bentuk teks dan multimedia (misalnya, klip video) dipublikasikan untuk konsumsi masyarakat umum atau audiens terbatas;
— anggota sebuah organisasi (seperti pegawai perusahaan, atau bentuk asosiasi lainnya dengan perusahaan);
— peran lain, di mana pengguna dapat diberikan peran secara tidak sengaja atau tanpa persetujuan mereka.

CONTOH 1 Ketika seorang pengguna mengunjungi situs yang memerlukan otorisasi, dan secara sengaja atau tidak sengaja memperoleh akses, pengguna tersebut dapat diberi label sebagai penyusup.

CONTOH 2 Seseorang bertindak sebagai pembeli atau penjual, dapat tanpa disadari berpartisipasi dalam transaksi kriminal penjualan barang curian atau aktivitas pencucian uang.

Organisasi sering menggunakan Internet untuk memublikasikan perusahaan dan informasi terkait, serta memasarkan produk dan layanan terkait. Organisasi juga memanfaatkan Internet sebagai bagian dari jaringannya untuk pengiriman dan penerimaan pesan elektronik (misalnya surel) dan dokumen lainnya (misalnya transfer fail).

Sejalan dengan prinsip yang sama untuk menjadi masyarakat korporasi yang baik, organisasi ini sebaiknya memperluas tanggung jawab korporasi mereka terhadap Internet dengan secara proaktif memastikan bahwa praktik dan tindakan mereka dalam penggunaan Internet tidak mengintroduksi risiko keamanan lebih lanjut ke dalam komunitas pengguna Internet.

Beberapa tindakan proaktif termasuk:
— manajemen keamanan informasi dengan mengimplementasikan dan mengoperasikan sistem manajemen keamanan informasi (ISMS) yang efektif (lihat ISO/IEC 27001 untuk persyaratan sistem manajemen keamanan informasi);
— mengimplementasikan kontrol berdasarkan ISO/IEC 27002 dan standar relevan lainnya, tanpa mengoperasikan ISMS;
— pemonitoran keamanan dan tanggap insiden;
— memasukkan keamanan sebagai bagian dari siklus hidup pengembangan perangkat lunak (SDLC), di mana level keamanan yang dibangun ke dalam sistem sebaiknya ditentukan berdasarkan kekritisan data organisasi;
— edukasi keamanan reguler bagi pengguna dalam organisasi melalui pembaruan teknologi dan proses yang berkelanjutan serta memantau perkembangan teknologi terkini; dan
— memahami dan menggunakan saluran yang tepat dalam berkomunikasi dengan vendor dan penyedia layanan tentang masalah keamanan yang ditemukan selama penggunaan.

7.3 Koordinator dan organisasi standardisasi

Koordinator dan organisasi standardisasi (ICANN, IETF, W3C dll.) mengembangkan standar teknis tentang penggunaan Internet dan layanan yang disediakan oleh penyedia layanan. Mereka memberi saran kepada organisasi mengenai peran dan tanggung jawab mereka di Internet.

7.4 Otoritas pemerintah

Pemerintah memegang informasi tentang isu keamanan nasional, strategis, militer, intelijen di antara banyak elemen lainnya yang berkaitan dengan pemerintah dan negara, tetapi juga informasi yang sangat luas mengenai individu, organisasi, dan masyarakat secara keseluruhan.

Pemerintah sebaiknya memproteksi infrastruktur dan informasi negaranya dari akses dan eksploitasi yang tidak sah. Terdapat tren yang sedang tumbuh dan berkembang tentang penawaran layanan pemerintahan elektronik menggunakan Internet. Hal ini merupakan saluran baru, di antara yang lainnya, untuk melancarkan serangan dan mengakses informasi tersebut di atas, yang jika berhasil, dapat menimbulkan dampak serius bagi suatu wilayah, pemerintah, dan masyarakatnya.

Otoritas pemerintah memainkan peran koordinasi antar-lembaga penegak hukum dan merupakan koordinator utama untuk menyebarkan informasi dan mengatur sumber daya yang disyaratkan, baik di tingkat nasional maupun korporasi, pada saat krisis yang timbul dari serangan siber yang masif. Hal ini juga termasuk otoritas seperti CERT dan organisasi serupa yang diberi tanggung jawab tersebut tergantung pada wilayah spesifik dalam konteksnya.

Pemerintah mengamanatkan program edukasi keamanan siber untuk universitas dan Sekolah Menengah Atas, dan memastikan bahwa kemitraan publik-swasta yang tepat diselenggarakan dengan struktur hukum yang diperlukan, yang mengatur lembaga penegak hukum dan mendefinisikan misi mereka.

7.5 Lembaga penegak hukum

Lembaga penegak hukum menegakkan regulasi dan meminta pertanggungjawaban semua pihak yang berkepentingan dalam hal kepatuhan mereka terhadap regulasi yang relevan dalam yurisdiksi nasionalnya.

7.6 Penyedia layanan Internet

Organisasi yang menyediakan layanan dapat termasuk dua kategori:
— penyedia akses ke Internet untuk pegawai dan mitra;
— penyedia layanan kepada konsumen Internet.

Layanan ini disediakan baik untuk komunitas tertutup (misalnya pengguna terdaftar), atau publik umum, melalui pengiriman aplikasi termasuk penyedia layanan *cloud* melalui Internet. Seorang konsumen juga dapat menjadi penyedia layanan, jika ia menyediakan layanan melalui Internet atau memungkinkan konsumen lain mengakses Internet.

Penyedia layanan juga dapat dipahami sebagai pembawa atau pedagang grosir, distributor lawan dan pengecer layanan akses. Perbedaan ini penting dari perspektif keamanan dan, khususnya, penegakan hukum. Jika distributor atau pengecer tidak dapat memberikan keamanan yang memadai atau akses yang sah, layanan dukungan sering kali kembali ke pembawa atau pedagang grosir. Penyedia layanan Internet (ISP) dapat memberikan dukungan dengan mengawasi “trafik” dan menyediakan rute atau hos alternatif untuk kontrol trafik. Mereka juga dapat mencari transfer "berbahaya" melalui Internet. Dengan otorisasi hukum yang diperlukan dan izin dari pengguna, mereka dapat memfilter apa yang berbahaya, seperti halnya solusi yang menyediakan “*sand boxes*” untuk memverifikasi perangkat perusak pada fail yang ditransfer. ISP dapat memperingatkan pelanggannya ketika mereka menemukan pola ancaman.

8 Asesmen dan penanganan risiko keamanan Internet

8.1 Umum

ISO 31000 menyediakan prinsip dan pedoman umum tentang manajemen risiko, sedangkan ISO/IEC 27005 menyediakan pedoman dan proses untuk manajemen risiko keamanan informasi dalam suatu organisasi, mendukung persyaratan ISMS menurut ISO/IEC 27001. Pedoman dan proses yang disediakan oleh dokumen-dokumen tersebut direkomendasikan untuk mengatasi manajemen risiko dalam konteks Internet. Merupakan tanggung jawab pihak yang berkepentingan untuk mendefinisikan pendekatan mereka terhadap manajemen risiko. Beberapa metodologi yang ada dapat digunakan berdasarkan kerangka kerja yang dideskripsikan dalam ISO/IEC 27005 untuk melakukan asesmen risiko dan mengelola risiko yang terkait dengan penggunaan Internet oleh organisasi, dengan mempertimbangkan ancaman dan kerentanan yang relevan serta masalah keamanan Internet.

Dalam organisasi di mana sumber daya yang tersedia terbatas, kontrol disyaratkan untuk mempertimbangkan rasionalitas antara kebutuhan organisasi terhadap keamanan dan sumber daya untuk menghindari kesalahan dalam pemilihan kontrol. Pemilihan kontrol yang tidak tepat dapat mengakibatkan risiko tambahan atau kontrol yang tidak efektif.

8.2 Ancaman

Agen ancaman (*threat agent*) adalah individu atau sekelompok individu yang mempunyai peran dalam pelaksanaan atau dukungan suatu serangan. Pemahaman menyeluruh tentang motif mereka (agama, politik, ekonomi, dll.), kapabilitas (pengetahuan, pendanaan, ukuran, dll.), dan intensi (kesenangan, kejahatan, spionase, dll.) sangat kritikal dalam asesmen kerentanan dan risiko, serta dalam pengembangan dan penerapan kontrol.

Perangkat perusak dapat mengakibatkan pembobolan terhadap kontrol keamanan (misalnya penangkapan dan pengungkapan kata sandi), pengungkapan informasi yang tidak diinginkan, perubahan informasi yang tidak diinginkan, penghancuran informasi, dan/atau penggunaan sumber daya sistem tanpa izin. Perangkat perusak biasanya dikirimkan melalui virus, *worm*, dan *trojan* dengan konsekuensi yang luas.

Virus adalah program yang dapat dieksekusi dan direplikasi yang memasukkan kodenya sendiri ke dalam program yang sah dengan tujuan merusak komputer hos (misalnya menghapus fail dan program, merusak penyimpanan dan sistem operasi). Dalam kondisi yang paling sederhana, *worm* adalah program komputer yang dimaksudkan untuk mereplikasi diri dan menyebar ke komputer lain melalui pesan keluar ke semua alamat di dalam daftar kontak pengguna untuk menguras sumber daya sistem. Selain itu, seperti halnya virus, *worm* dapat menyebarkan kode yang dapat merusak hos. Kode tersebut disebut sebagai muatan (*payload*) (misalnya kemampuan untuk mengenkripsi fail dalam perangkat pemeras (*ransomware*) dan instalasi pintu belakang sistem yang memungkinkan akses jarak jauh). *Trojan* adalah program jahat yang menyamar atau tertanam dalam perangkat lunak sah yang memiliki tujuan serupa dengan virus dan worm, namun, tidak seperti keduanya, *trojan* tidak mereplikasi atau menyebar dengan sendirinya.

Ancaman keamanan Internet terhadap informasi identifikasi pribadi (PII) pengguna Internet utamanya berkisar pada masalah identitas, yang disebabkan oleh kebocoran atau pencurian informasi pribadi. Jika identitas daring seseorang dicuri atau disamarkan, orang tersebut dapat kehilangan akses ke layanan dan aplikasi utama. Dalam skenario yang lebih serius, konsekuensinya dapat berkisar dari insiden finansial hingga level nasional. Akses tidak sah terhadap informasi keuangan seseorang juga membuka kemungkinan terjadinya pencurian uang dan penipuan.

CONTOH 1 Informasi kredit dapat dijual di pasar gelap atau *dark net*, yang dapat memfasilitasi pencurian identitas daring.

CONTOH 2 Contoh ancaman lain yang juga setara dengan ancaman terhadap kehidupan adalah perundungan siber, penguntitan daring, dan kejahatan eksploitasi, termasuk eksploitasi anak, dan perdagangan manusia.

Ancaman lainnya adalah kemungkinan bahwa titik akhir termasuk perangkat pribadi dan bawa perangkat anda sendiri (*bring your own device* – BYOD) dijadikan *zombie* atau bot. Perangkat komputasi dapat terbobol dan karenanya menjadi bagian dari *botnet* yang lebih besar. Kehadiran daring dan bisnis daring suatu organisasi sering kali menjadi sasaran penjahat yang intensinya lebih dari sekadar kenakalan.

Dalam skala yang lebih besar, infrastruktur yang mendukung Internet dapat juga dijadikan target. Meskipun hal ini tidak mempengaruhi fungsi Internet secara permanen, hal ini mempengaruhi reliabilitas dan ketersediaan infrastruktur, yang berkontribusi pada keamanan Internet.

Pada level nasional atau internasional, Internet merupakan area di mana perilaku ilegal tumbuh subur di yurisdiksi tertentu. Karena sifat dari Internet, secara spesifik adalah tantangan dalam mendefinisikan batasan dan pembatas, sulit untuk mengatur dan mengontrol cara penggunaannya.

Penjahat dapat secara sah membeli aplikasi, layanan, dan sumber daya yang memfasilitasi tujuan mereka, atau mereka dapat menggunakan cara ilegal untuk mengamankan sumber daya tersebut untuk menghindari deteksi dan pelacakan. Hal ini dapat mencakup perolehan sumber daya komputasi besar-besaran melalui *botnet*.

Ancaman lainnya berkaitan dengan modifikasi yang disengaja atas informasi yang tersedia secara publik atau informasi hak milik, atau pembuatan informasi palsu dan hoaks yang, jika diandalkan, dapat menimbulkan kerugian serius.

8.3 Kerentanan

Kerentanan adalah kelemahan suatu aset atau kontrol yang dapat dieksploitasi oleh suatu ancaman. Produsen, pengembang perangkat lunak, dan pengembang teknologi lainnya menghasilkan pembaruan dan *patch* keamanan untuk memperbaiki kelemahan tersebut setelah ditemukan dan diatasi. Saat sistem menerima *patch*, pembaruan atau elemen baru ditambahkan. Ketika sistem menjadi usang atau tidak didukung oleh vendor atau tidak dilakukan *patch* ke versi terbaru, kerentanan baru dapat muncul. Pihak yang berkepentingan sebaiknya memiliki pengetahuan dan pemahaman menyeluruh tentang aset atau kontrol yang dipermasalahkan, seperti halnya dengan ancaman, agen ancaman, dan risiko yang terlibat, agar dapat melakukan asesmen yang komprehensif. Pihak yang berkepentingan sebaiknya waspada terhadap kerentanan *zero-day* di mana *patch* untuk kerentanan tersebut tidak tersedia.

Aplikasi web yang diakses melalui Internet rentan terhadap berbagai kerentanan yang disebabkan oleh desain yang buruk, kode yang ditulis dengan buruk, dan pengembangan yang buruk terhadap *libraries* dan *executables* produksi. Contoh kerentanan tersebut termasuk *bypass* otentikasi, serangan injeksi basis data, dan serangan skrip lintas situs (*cross-site scripting attack*). Dalam serangan tersebut, permintaan dapat dimanipulasi untuk menyalahgunakan fungsi server web.

8.4 Vektor serangan

Vektor serangan adalah jalur atau cara yang melaluinya penyerang dapat memperoleh akses ke komputer atau server jaringan sehingga memberikan manfaat yang merusak.

Pemindai port adalah salah satu alat tertua dan masih sangat efektif digunakan oleh penyerang. Mereka memindai semua port yang tersedia pada sistem hadap-Internet untuk mengonfirmasi port mana yang terbuka. Ini biasanya merupakan salah satu langkah pertama yang dilakukan oleh calon penyerang pada target sistem hadap-Internet. Meskipun serangan awal selalu menargetkan sistem yang dapat dilihat secara publik (misalnya *router*, server, *firewall*, situs web, dll.), penyerang juga dapat berupaya untuk mengeksploitasi aset yang berada di dalam jaringan privat yang terhubung ke sistem yang dapat dilihat secara publik tersebut.

Mendengarkan saluran komunikasi adalah vektor serangan yang sederhana dan mudah. Ini juga adalah salah satu yang tertua. Menyalin dan menganalisis trafik dapat sangat berguna untuk mendeteksi titik masuk dan memulai vektor ancaman lainnya. Penyerang juga dapat menggunakan pembajakan komunikasi (dengan mengekor (*tailgating*) atau membonceng (*piggy-backing*)) dan menyamarkan dirinya di balik identitas atau kredensial, dan dengan mengorbankan pengguna yang sah tanpa sepengetahuan mereka.

Banyak serangan di Internet dilakukan dengan menggunakan perangkat perusak, seperti perangkat pengintai, *worm*, dan virus. Informasi sering kali dikumpulkan melalui teknik *phishing*. Suatu serangan dapat terjadi sebagai vektor serangan tunggal atau dilakukan sebagai serangan bauran atau serangan bertarget. Serangan-serangan tersebut dapat disebarkan melalui, misalnya, situs web yang mencurigakan, unduhan yang tidak terverifikasi, surel *spam*, eksploitasi jarak jauh, eksploitasi *zero-day*, dan *removable media* yang terinfeksi.

Mekanisme lain yang semakin berkembang dalam penggunaan dan kecanggihan, untuk melakukan serangan, adalah mekanisme yang berbasis pada situs jejaring sosial dan penggunaan fail yang korup pada situs web yang sah. Situs web yang sah juga dapat diretas dan beberapa failnya menjadi korup dan digunakan sebagai sarana untuk melakukan serangan. Individu cenderung secara implisit mempercayai situs web yang sering dikunjungi. Penyerang dapat menerapkan teknik *waterhole* untuk membobol kelompok pengguna akhir yang spesifik dengan menginfeksi situs web yang sering dikunjungi. Selain serangan yang dilancarkan oleh penyerang manusia, komputer yang terinfeksi perangkat perusak juga melancarkan berbagai serangan ke komputer yang terhubung di sekitarnya.

Dengan proliferasi aplikasi *peer-to-peer*, yang biasa digunakan untuk berbagi fail seperti musik digital, video, foto, dll., penyerang menjadi semakin canggih dalam menyamarkan dirinya dan kode berbahaya mereka dengan menggunakan fail yang dipertukarkan sebagai *Trojan* untuk serangan mereka. Ketika seorang penyerang, melalui pencurian identitas, dapat menyamarkan dirinya sebagai kontak yang sah, penyerang dapat melibatkan orang lain, dan jalan baru terbuka untuk melancarkan berbagai jenis serangan.

Teknik lainnya adalah pemalsuan (*spoofing*) IP, di mana penyerang memanipulasi alamat IP yang terkait dengan pesan mereka dalam upaya untuk menyamarkannya sebagai sumber yang dikenal dan tepercaya, sehingga mendapatkan akses tidak sah ke sistem.

Penyerang tidak selalu menggunakan vektor serangan yang sama. Penyerang menggunakan banyak vektor dan sering mengubahnya. Beberapa serangan disembunyikan sedemikian rupa sehingga tidak terdeteksi sampai sudah terlambat bagi pengguna. *Defender* sebaiknya mempertimbangkan hal ini dan mencari pertahanan terhadap berbagai vektor dan bukan hanya vektor yang telah digunakan untuk melawan mereka.

Perangkat IoT, ponsel pintar, dll. dapat dihubungkan ke Internet. Perangkat tersebut dapat bertindak sebagai vektor serangan tambahan sama seperti perangkat terhubung-Internet lainnya, jika perangkat tersebut tidak dikontrol secara memadai saat terhubung ke jaringan organisasi.

Ancaman persisten tingkat lanjut (APT) adalah metode serangan dengan tujuan mencuri informasi dalam jangka waktu yang lama di mana penyerang mendapatkan akses berkelanjutan ke jaringan organisasi, membuat dirinya tidak terdeteksi, bergerak secara lateral, melihat, mempelajari, dan tetap berada di jaringan.

Metode serangan lama lainnya adalah serangan *brute force*. Metode ini menggunakan percobaan untuk menebak kredensial *login*, kunci enkripsi, menemukan halaman web tersembunyi di mana penyerang bekerja melalui semua kemungkinan kombinasi dengan harapan dapat menebak dengan benar untuk mendapatkan akses ke jaringan dan informasi organisasi.

9 Pedoman keamanan Internet

9.1 Umum

Pihak yang berkepentingan dapat menilai risiko dengan mempertimbangkan ancaman yang diterapkan pada aset mereka. Analisis ini dapat membantu dalam pemilihan kontrol untuk menangani risiko dan menguranginya ke level yang dapat diterima. Kontrol diimplementasikan untuk mengurangi kemungkinan atau akibat dari risiko tersebut, dan untuk memenuhi persyaratan keamanan pihak yang berkepentingan (baik secara langsung maupun tidak langsung dengan memberikan arahan kepada pihak lain).

Kerentanan dapat tetap ada setelah implementasi kontrol. Kerentanan tersebut dapat dieksploitasi oleh agen ancaman. Pihak yang berkepentingan berupaya meminimalkan risiko, dengan mempertimbangkan kendala lainnya. Pihak yang berkepentingan sebaiknya yakin bahwa kontrol tersebut memadai untuk melawan ancaman terhadap aset sebelum mereka membiarkan aset terkena ancaman tertentu. Jika pihak yang berkepentingan tidak memiliki kapabilitas untuk mengevaluasi seluruh aspek kontrol, mereka dapat melakukan evaluasi kontrol dengan menggunakan organisasi eksternal.

Cara efektif untuk menghadapi risiko keamanan Internet adalah dengan melibatkan kombinasi berbagai strategi, dengan mempertimbangkan berbagai pihak yang berkepentingan.

Strategi tersebut meliputi:
— pendekatan spesifik industri, dengan kolaborasi semua pihak yang berkepentingan untuk mengidentifikasi dan mengatasi permasalahan dan risiko Internet;
— edukasi konsumen dan pegawai secara luas, menyediakan sumber daya tepercaya mengenai cara mengidentifikasi dan mengatasi risiko Internet spesifik dalam organisasi serta komunitas pengguna Internet;
— solusi teknologi yang inovatif untuk membantu memproteksi konsumen dari serangan berbasis Internet, agar tetap mengikuti perkembangan terkini dan bersiap menghadapi eksploitasi baru;
— pembaruan undang-undang dan peraturan sehingga memungkinkan keadilan ditegakkan di berbagai yurisdiksi.

9.2 Kontrol keamanan Internet

9.2.1 Umum

Sebagian besar organisasi menggunakan Internet untuk berbagai tujuan, mulai dari menjelajahi web, *blogging*, berjejaring sosial dan mengakses layanan *cloud* publik, hingga berbagi informasi dan melakukan bisnis perdagangan elektronik (*e-commerce*). Hal ini melibatkan berbagi informasi bisnis rahasia termasuk informasi pribadi saat melakukan transaksi daring. Internet sebagai jaringan publik rentan terhadap ancaman unik tertentu. Jika tidak diatasi, ancaman ini akan mengakibatkan serangan yang sulit dikelola.

Organisasi sebaiknya mengembangkan kebijakan, prosedur, dan kapabilitas respons untuk:
a) mendefinisikan aturan penggunaan Internet yang sesuai aturan (*acceptable use*) bagi personel;
b) mendefinisikan layanan apa yang dapat diekspos melalui Internet;
c) mengidentifikasi ancaman, kerentanan, vektor serangan dan risiko yang terkait;
d) mendefinisikan peran dan tanggung jawab berbagai pengguna Internet;
e) meningkatkan kesadaran pengguna tentang praktik penggunaan Internet yang aman;
f) menentukan departemen yang bertanggung jawab untuk menangani masalah keamanan Internet;
g) menetapkan mekanisme respons terhadap insiden keamanan siber;
h) melakukan latihan keamanan untuk menguji mekanisme respons terhadap serangan yang berasal dari Internet.

Berdasarkan asesmen risiko, seseorang dapat mengungkap berbagai risiko keamanan Internet yang relevan yang dapat diatasi melalui berbagai pengendalian seperti yang dijelaskan di bawah ini.

9.2.2 Kebijakan keamanan Internet

Organisasi sebaiknya menyiapkan dan memublikasikan kebijakan mengenai penggunaan Internet oleh personel dan pihak terkait lainnya sejalan dengan tujuan keamanan. Hal ini menentukan layanan Internet mana yang digunakan, siapa yang berwenang menggunakannya, dan apa tujuan keamanannya. Kebijakan ini mengarahkan semua pedoman lainnya untuk koneksi yang aman ke, dan penggunaan dari, Internet.

Kebijakan keamanan Internet sebaiknya didefinisikan, disetujui oleh manajemen, dipublikasikan dan dikomunikasikan kepada, dan diakui oleh, personel terkait, kontraktor, dan pihak eksternal. Kebijakan keamanan Internet sebaiknya menetapkan personel yang diberi wewenang untuk mengakses Internet, konten yang dapat mereka lihat, perilaku yang dilarang di Internet, di antara yang lain. Tanggung jawab sebaiknya dialokasikan untuk semua aktivitas yang berkaitan dengan Internet, dan untuk desain, persetujuan, implementasi, pengoperasian dan pemonitoran semua kontrol spesifik yang berlaku untuk keamanan Internet.

ISO/IEC 27002 memberikan panduan lebih lanjut mengenai kebijakan keamanan Internet.

9.2.3 Kontrol akses

Kontrol akses mencakup hak akses tidak hanya untuk pengguna, tetapi juga entitas lain seperti perangkat, aplikasi, atau proses otomatis. Oleh karena itu, setiap koneksi sebaiknya diautentikasi, dan setiap aktivitas diberi wewenang sebagaimana mestinya, berdasarkan peran dan izin yang ditetapkan sesuai dengan aturan bisnis dan keamanan, dan setiap entitas sebaiknya diberi izin dengan hak privilese paling rendah. Hal ini meningkatkan ketertelusuran akses terhadap informasi dan aset, serta mengurangi anonimitas untuk meningkatkan keamanan.

Aturan untuk mengontrol akses fisik dan logis terhadap informasi dan aset adalah bahwa aset lain yang terkait dengan Internet dan fasilitas pemrosesan informasi sebaiknya ditetapkan dan diimplementasikan berdasarkan nilai bisnis dan informasi. Aturan mengenai akses terhadap informasi dan aset penting adalah bahwa aset lain yang terkait dengan informasi dan fasilitas pemrosesan informasi sebaiknya sejalan dengan kebijakan kontrol akses dan kebijakan klasifikasi informasi yang ditetapkan.

Akun sebaiknya dibatasi hanya untuk pengguna yang diberi otorisasi disebabkan oleh peran atau fungsi pekerjaannya. Setiap pengguna sebaiknya memiliki akun terpisah dan tidak boleh dibagikan, dan kata sandi yang sama juga tidak boleh digunakan untuk lebih dari satu akun.

Hak akses terhadap informasi, sistem, aplikasi dan layanan sebaiknya ditetapkan, ditinjau, disesuaikan, dimodifikasi, dan dihapus sesuai dengan kebijakan dan prosedur organisasi mengenai kontrol akses. Alokasi dan penggunaan hak akses privilese (*privileged*) sebaiknya dibatasi dan dikontrol. Teknologi dan prosedur otentikasi yang aman sebaiknya diimplementasikan berdasarkan pembatasan akses informasi dan aturan kontrol akses terkait. Sistem manajemen kata sandi sebaiknya diterapkan untuk mengelola dan mendukung proses pembuatan kata sandi dan mutu daripadanya.

Sistem informasi yang terhubung langsung ke Internet (misalnya infrastruktur *firewall*, perangkat perimeter jaringan, dll.) dapat memiliki satu atau lebih program utilitas istimewa yang mampu mengambil alih kontrol sistem dan aplikasi. Jika penyerang mendapatkan akses ke salah satu sistem, maka program utilitas yang memiliki hak privilese ini, jika tidak dikontrol dengan benar, dapat mengakibatkan akses privilese diperoleh penyerang.

Program ini sebaiknya dikontrol secara memadai oleh organisasi sehingga penyusup tidak mendapatkan akses ke program utilitas privilese tersebut dan mengambil alih kontrol sistem dan aplikasi. Manajemen akses yang efektif sebaiknya mencakup:
— tinjauan berkala terhadap semua hak akses;
— tinjauan berkala terhadap log administratif.

ISO/IEC 27002 dan ISO/IEC 29146 memberikan panduan lebih lanjut mengenai manajemen akses.

9.2.4 Edukasi, kesadaran, dan pelatihan

Personel organisasi (termasuk manajemen puncak, admin sistem, staf TI, dan pengguna yang memiliki hak privilese, dll.) sebaiknya diberi informasi terbaru secara berkala tentang ancaman utama (misalnya *phishing* dan *vishing*) dan tindakan yang diambil untuk mencegahnya dan merespons jika terjadi tindakan yang tidak tepat.

Banyak ancaman baru yang diluncurkan di Internet setiap hari dan terus berkembang serta menjadi lebih senyap dan canggih. Ketika mengimplementasikan kontrol untuk melawan serangan, ada kemungkinan pengguna tidak menyadari bahwa mereka adalah korban serangan yang baru atau yang lebih canggih.

Organisasi sebaiknya menyediakan materi kesadaran dan pelatihan secara berkala bagi personel dengan menggunakan berbagai format seperti komunikasi surel, pelatihan daring, dan pengiriman pesan melalui intranet, untuk menginformasikan personel tentang ancaman daring serta kewajiban mereka atas pelaporan insiden dan penggunaan yang dapat diterima. Hal ini memberikan level pemahaman dan menarik perhatian mereka untuk memproteksi diri mereka sendiri dan organisasi.

ISO/IEC 27002 memberikan panduan lebih lanjut mengenai edukasi, kesadaran, dan pelatihan.

9.2.5 Manajemen insiden keamanan

Insiden keamanan di Internet dapat berkisar dari berbagai macam serangan siber terhadap sumber daya organisasi yang hadap-Internet, serta server, basis data, dan aplikasi yang berada di belakang sumber daya yang terhubung ke Internet. Insiden keamanan dapat dipicu dari mana saja di Internet. Terkadang hos yang melakukan serangan dapat menjadi hos yang terbobol. Beberapa insiden dapat bersifat rumit dan memerlukan keterampilan khusus untuk memberikan respons yang memadai. Insiden sering kali melintasi batas negara, geografis, dan organisasi, dan kecepatan arus informasi serta perubahan dari insiden yang sedang terjadi sering kali memberikan waktu yang terbatas bagi individu dan organisasi yang merespons untuk bertindak.

Tim manajemen insiden (IMT) dengan tim tanggap insiden (IRT) pendukung sebaiknya dibentuk untuk memberikan organisasi kapabilitas dalam menilai, merespons, dan belajar dari insiden tersebut. Prosedur tanggap insiden sebaiknya mempertimbangkan pendeteksian dan pelaporan terjadinya peristiwa keamanan seperti insiden potensial dan aktual yang dilakukan oleh manusia atau sarana otomatis. Alat pemonitoran yang diimplementasikan oleh organisasi dapat mendeteksi dan mengirimkan peristiwa keamanan untuk tanggap insiden. Inteligensi ancaman adalah informasi tentang ancaman dan pelaku ancaman yang membantu memitigasi peristiwa berbahaya di dunia maya. Personel keamanan informasi sebaiknya terus memindai sumber inteligensi ancaman seperti inteligensi media sosial, inteligensi manusia, inteligensi teknis, atau inteligensi dari web yang dalam dan gelap, mengumpulkan informasi, kemudian menganalisisnya.

Solusi teknis untuk mendukung berbagi informasi dan koordinasi sebaiknya ditetapkan untuk membantu mempersiapkan dan merespons peristiwa keamanan dan insiden siber. Ini adalah langkah penting yang sebaiknya diambil organisasi sebagai bagian dari kontrol keamanan mereka. Solusi tersebut sebaiknya melibatkan berbagi informasi dan koordinasi yang aman, efektif, reliabel, dan efisien.

Insiden yang berkaitan dengan keamanan Internet sebaiknya ditanggapi oleh kontak yang ditunjuk dan orang-orang relevan lainnya dalam organisasi atau pihak yang berkepentingan. Setiap persyaratan eksternal mengenai pelaporan insiden kepada pihak berkepentingan yang relevan dalam jangka waktu yang ditentukan (misalnya persyaratan pemberitahuan insiden kepada regulator dalam jangka waktu yang ditentukan) sebaiknya dipertimbangkan ketika mengimplementasikan prosedur manajemen insiden. Organisasi sebaiknya membangun dan memelihara kontak dengan otoritas hukum, regulasi, dan pengawasan yang relevan. Organisasi tersebut juga sebaiknya menjaga kontak dengan kelompok kepentingan khusus serta forum keamanan khusus dan asosiasi profesional lainnya.

Ada kebutuhan untuk berbagi informasi, koordinasi, dan penanganan insiden yang efisien dan efektif di antara pihak-pihak yang berkepentingan dalam keamanan Internet. Kolaborasi ini sebaiknya dilakukan dengan cara yang aman dan reliabel yang juga memproteksi privasi individu terkait. Banyak pihak yang berkepentingan dapat tinggal di lokasi geografis dan zona waktu yang berbeda dan kemungkinan besar diatur oleh persyaratan regulasi yang berbeda.

Berbagi informasi dan kolaborasi termasuk:
— elemen penting dari pertimbangan untuk membangun kepercayaan;
— proses yang diperlukan untuk kolaborasi serta pertukaran dan berbagi informasi;
— persyaratan teknis untuk integrasi dan interoperabilitas sistem di antara berbagai pihak yang berkepentingan.

Organisasi yang menggunakan Internet sebaiknya mendefinisikan dan menerapkan prosedur untuk identifikasi, pengumpulan, akuisisi, dan penyimpanan informasi, yang dapat berfungsi sebagai bukti jika terjadi insiden keamanan. Diharapkan agar bukti dikumpulkan dengan cara yang dapat diterima di pengadilan nasional atau otoritas internasional jika insiden tersebut terbukti berasal dari negara lain sesuai dengan catatan pemonitoran dan bukti digital lainnya.

Bukti digital dapat melampaui batas-batas organisasi atau yurisdiksi jika terjadi insiden keamanan. Dalam kasus seperti ini, sebaiknya dipastikan bahwa organisasi berhak mengumpulkan informasi yang disyaratkan sebagai bukti digital untuk tindakan di masa depan. Pengaturan jam komputer yang benar adalah penting untuk memastikan akurasi catatan audit, yang diharapkan dapat digunakan untuk investigasi jika terjadi serangan dari Internet atau diharapkan sebagai bukti dalam kemungkinan tindakan hukum.

Informasi yang diperoleh dari evaluasi insiden keamanan sistem hadap-Internet sebaiknya digunakan untuk mengidentifikasi insiden yang berulang atau terkait untuk merencanakan dan mengimplementasikan perubahan guna mengurangi kemungkinan atau dampak insiden serupa di masa depan. Alat seperti IPS dan SIEM dapat dikonfigurasi ulang berdasarkan evaluasi insiden keamanan dan amandemen kebijakan yang relevan dapat dimulai untuk mencegah insiden di masa depan.

ISO/IEC 27002 dan seri ISO/IEC 27035 memberikan panduan lebih lanjut tentang manajemen insiden.

9.2.6 Manajemen aset

Komponen TIK yang berisi informasi dan aplikasi kritikal sebaiknya diidentifikasi. Secara tradisi, organisasi diharapkan mengetahui di mana aset mereka berada secara fisik untuk memproteksinya secara memadai. Organisasi tidak hanya menyimpan inventaris aset TIK terkini dalam kendali mereka tetapi juga memelihara daftar aset informasi di mana informasi mereka diproses, disimpan, ditransfer, baik di jaringan internal mereka atau menggunakan *cloud*/*hosting solution* berbasis Internet. Dengan cara ini, organisasi dapat mengelola risiko terhadap informasi mereka di mana pun itu berada dan membuat keputusan berdasarkan-risiko mengenai apakah tepat untuk informasi tersebut disimpan di luar lingkungan kontrol organisasi. Demikian pula, untuk komponen jaringan, organisasi diharapkan mengetahui di mana aset sensitif berada sehubungan dengan titik masuk untuk calon penyerang. Ini dapat berupa akses Internet resmi — melalui *firewall* — dan semua koneksi lain dengan perangkat, (misalnya ponsel cerdas, IoT). Organisasi juga sebaiknya mengidentifikasi jalur kritikal yang digunakan untuk mengakses aset TIK yang sensitif atau untuk mengirimkan informasi sensitif dalam jaringan organisasi. Jalur ini tidak boleh terlihat, dapat diakses, atau dipantau oleh penyusup. Tanpa pengetahuan ini, pemisahan jaringan yang memadai tidak mungkin dilakukan. Inventarisasi ini sebaiknya berupa arsitektur jaringan (lokasi fungsionalitas) dan infrastruktur, keduanya secara jelas menunjukkan titik masuk/koneksi dengan Internet (semua jaringan yang saling terhubung).

Aturan penggunaan yang dapat diterima dan prosedur penanganan aset adalah bahwa aset lain yang terkait dengan Internet dan fasilitas pemrosesan terkait sebaiknya diidentifikasi, didokumentasikan, dan diimplementasikan. Organisasi sebaiknya memiliki dan menggunakan prosedur untuk mengevaluasi pentingnya informasi dan aset TIK yang menyimpan dan mentransfernya. Hal ini akan memungkinkan organisasi untuk mengidentifikasi dengan jelas apa yang sebaiknya diproteksi dan pada level apa dalam hal kebijakan umum dan keamanan jaringan.

ISO/IEC 27002 memberikan panduan lebih lanjut tentang manajemen aset.

9.2.7 Manajemen pemasok

Proses dan prosedur sebaiknya diidentifikasi dan diimplementasikan untuk mengelola risiko keamanan Internet yang terkait dengan penggunaan pemasok. Semua persyaratan keamanan informasi yang relevan sebaiknya ditetapkan dan disetujui oleh masing-masing pemasok berdasarkan jenis pemasok dan risiko terkait. Manajemen risiko dalam kaitannya dengan pemasok TIK dan informasi yang mereka simpan, eksploitasi, atau dapat mereka akses, merupakan kunci dalam mempersiapkan kontrak yang memastikan bahwa tujuan keamanan informasi organisasi terus tercapai.

Perjanjian dengan pemasok yang terkait dengan Internet (seperti ISP dan penyedia layanan *cloud* melalui Internet) sebaiknya dibuat dan didokumentasikan untuk memastikan bahwa ada pemahaman yang jelas antara organisasi dan pemasok mengenai kewajiban kedua belah pihak untuk memenuhi persyaratan keamanan informasi yang relevan. Organisasi sebaiknya menjalin kemitraan terbuka dengan ISP, penyedia layanan telekomunikasi, penyedia layanan *cloud*, dan mitra untuk menginformasikan/memperingatkan deteksi ancaman yang masuk. Kemampuan penyedia layanan Internet untuk mengelola layanan yang disepakati dengan cara yang aman sebaiknya ditentukan dan dimonitor secara berkala. Diharapkan organisasi dan penyedia layanan mencapai kesepakatan mengenai hak untuk mengaudit.

Untuk layanan *cloud* yang dapat diakses melalui Internet dan sebagaimana yang dilanggan oleh organisasi, organisasi diharapkan meninjau dan menegosiasikan perjanjian layanan *cloud* dengan penyedia layanan *cloud*. Organisasi sebaiknya melakukan penilaian risiko yang relevan untuk mengidentifikasi risiko yang terkait dengan penggunaan layanan *cloud* dan mengelola risiko selama jangka waktu perjanjian. Perjanjian layanan *cloud* diharapkan dapat memenuhi persyaratan kerahasiaan, integritas, ketersediaan, dan penanganan PII organisasi. Untuk setiap layanan *cloud* di mana organisasi tidak dapat menegosiasikan ketentuan perjanjian, diharapkan organisasi memasuki perjanjian dengan mata terbuka lebar, memahami risiko penggunaan layanan dan cara mengelola risiko ini selama jangka waktu perjanjian.

Perangkat berbasis *cloud* seperti alat rapat web, alat obrolan web, dan alat penyimpanan *cloud* menimbulkan risiko bagi organisasi jika alat ini memiliki *bug* keamanan bawaan yang dapat dieksploitasi oleh pelaku kejahatan, sehingga penting bagi organisasi untuk menetapkan kontrol keamanan bagi penggunaan alat berbasis *cloud* ini.

Hal-hal berikut dapat dipertimbangkan untuk dimasukkan dalam perjanjian guna memenuhi persyaratan keamanan Internet yang teridentifikasi:

a) persyaratan hukum dan regulasi, termasuk persyaratan proteksi informasi di ujung ISP seperti proteksi dari DDoS dan serangan lainnya;
b) kewajiban masing-masing pihak dalam kontrak untuk mengimplementasikan serangkaian kontrol yang disepakati termasuk kontrol akses, pemonitoran jaringan dan sistem, pelaporan dan audit; serta kewajiban pemasok untuk mematuhi persyaratan keamanan organisasi
c) persyaratan dan prosedur manajemen insiden (khususnya pemberitahuan dan kolaborasi selama remediasi insiden);
d) pemonitoran, peninjauan, dan manajemen perubahan layanan pemasok untuk memastikan bahwa syarat dan ketentuan keamanan informasi pada perjanjian dipatuhi, dan memungkinkan pemonitoran level kinerja layanan untuk memverifikasi kepatuhan terhadap perjanjian, memonitor perubahan yang dilakukan oleh pemasok, dan memonitor perubahan dalam layanan pemasok.

ISO/IEC 27002, seri ISO/IEC 27036, ISO/IEC TR 23187, dan ISO/IEC 27017 memberikan panduan lebih lanjut terkait pemasok.

9.2.8 Keberlangsungan bisnis melalui Internet

Beberapa aktivitas bisnis seperti perdagangan berbasis Internet dan aktivitas perdagangan elektronik (*e-commerce*) lainnya bergantung pada infrastruktur Internet organisasi di dalam organisasi. Gangguan pada layanan Internet dapat disebabkan oleh serangan DoS dan DDoS dari pelaku kejahatan, kerusakan perangkat perimeter, atau setiap gangguan dari ujung ISP. Serangan DoS dan DDoS juga dapat dilakukan oleh pelaku kejahatan di pihak ISP yang dapat mengakibatkan pemadaman total pada *Internet backbone*. Fasilitas pemrosesan informasi sebaiknya diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan.

Setiap gangguan pada infrastruktur Internet membentuk risiko keberlangsungan organisasi dan sebaiknya diatasi oleh organisasi. Organisasi sebaiknya merencanakan pengadaan layanan Internet dari ISP yang berbeda untuk langkah-langkah keberlangsungan dasar. Organisasi sebaiknya menerapkan langkah-langkah keamanan untuk menghindari gangguan seperti tindakan anti-DDoS untuk keberlangsungan perangkat jaringan. Organisasi juga dapat mensyaratkan masing-masing ISP untuk menerapkan tindakan anti-DDoS dalam jaringan ISP. Terlepas dari layanan keberlangsungan, organisasi sebaiknya terus mempertimbangkan keamanan informasi dalam setiap solusi bahkan ketika dalam mode keberlangsungan bisnis.

ISO/IEC 27002, ISO 22301, dan ISO/IEC 27031 memberikan panduan lebih lanjut terkait keberlangsungan TIK.

9.2.9 Proteksi privasi melalui Internet

Sebagian besar penyedia layanan mengontrol atau memproses PII. Ketika informasi ini digunakan untuk tujuan yang berbeda dengan kepentingan pemilik data, masalah privasi akan muncul. Penyedia layanan *hosting* memproses PII di jaringan dan pusat data mereka sebagai bagian dari layanan bisnis mereka. Layanan ini, yang mencakup situs web dan aplikasi online lainnya, sering kali dikemas ulang dan dijual kembali oleh pelanggan *hosting* ke konsumen lain, seperti usaha kecil dan pengguna akhir, serta dibuat dapat diakses melalui Internet.

Jika pelanggan *hosting* menyiapkan server yang tidak aman, atau membawakan konten berbahaya di situs atau aplikasi mereka, keamanan konsumen termasuk PII yang disimpan oleh aplikasi daring tersebut, akan terkena dampak buruk. Oleh karena itu, penting agar layanan, setidaknya, memenuhi standar praktik terbaik dengan mematuhi persyaratan perjanjian minimum yang mencakup persyaratan privasi pengguna. Sebagai tambahan pada ketentuan proteksi data dan privasi personal di situs atau aplikasi hadap-Internet, penyedia layanan sebaiknya mensyaratkan situs atau aplikasi yang dibawakan di jaringan mereka untuk mengimplementasikan serangkaian kontrol keamanan praktik terbaik di level aplikasi sebelum diluncurkan. Sebelum mendaftar ke layanan di Internet, organisasi sebaiknya melakukan asesmen dampak privasi (*privacy impact assessment* / PIA) untuk mengidentifikasi informasi pribadi yang dapat digunakan, dikumpulkan, diproses, disimpan, atau dikirimkan dan risiko privasi terkait untuk menentukan apakah informasi tersebut dapat diterima oleh organisasi dan mengelolanya sebagaimana mestinya. Hal ini tidak hanya mencakup pengumpulan data pelanggan untuk menyediakan layanan tetapi juga dapat mencakup pengumpulan metadata seperti alamat IP atau data geolokasi individu yang menjelajahi situs web. Organisasi sebaiknya memublikasikan pemberitahuan privasi di situs mereka untuk menginformasikan dengan jelas kepada semua penggunanya tentang persyaratan berinteraksi dengan layanan daring organisasi. Penyembunyian data (*data masking*) sebaiknya digunakan sesuai dengan kebijakan organisasi mengenai kontrol akses dan persyaratan bisnis, dengan mempertimbangkan persyaratan hukum. Tindakan DLP sebaiknya diterapkan pada sistem dan jaringan yang memproses, menyimpan, atau mengirimkan informasi sensitif. Terdapat fitur teknologi di beberapa peramban Internet, yang memungkinkan pengaturan privasi diubah oleh pengguna.

ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29100, dan ISO/IEC 27018 memberikan panduan lebih lanjut terkait privasi.

9.2.10 Manajemen kerentanan

Informasi tentang kerentanan sistem TIK yang digunakan sebaiknya diperoleh tepat waktu. Paparan organisasi terhadap kerentanan tersebut sebaiknya dievaluasi dan tindakan yang tepat sebaiknya diambil untuk mengatasi risiko terkait. Konfigurasi, termasuk konfigurasi keamanan perangkat keras, perangkat lunak, layanan dan jaringan sebaiknya dibuat, didokumentasikan, diimplementasikan, serta dimonitor dan ditinjau.

Organisasi yang memasok produk (*firewall*, IDS, IPS, dll.) dan layanan (layanan jaringan, layanan VoIP, layanan keamanan terkelola, dll.) teknologi sebaiknya secara konsisten dan efektif mengimplementasikan langkah-langkah untuk mengidentifikasi, menangani, dan mengungkapkan kerentanan produk dan layanan yang mereka pasok. Berdasarkan kerentanan yang diungkapkan oleh vendor produk dan layanan, tindakan proteksi yang tepat diimplementasikan untuk mengatasi kerentanan tersebut.

Dengan meningkatnya penyebaran perangkat perusak di Internet, organisasi penyedia layanan dapat menerima laporan terkait infeksi perangkat perusak dan perangkat pengintai serta masalah keamanan lainnya. Informasi tersebut penting dan berguna bagi vendor terkait untuk menilai risiko infeksi perangkat perusak, dan memberikan pembaruan pada alat yang diperlukan untuk memastikan bahwa perangkat perusak atau perangkat pengintai baru yang terdeteksi dapat dihapus atau dinonaktifkan secara efektif. Dalam hal ini, organisasi sebaiknya menjalin kontak dengan vendor keamanan dan menyerahkan laporan dan sampel perangkat perusak yang relevan kepada vendor untuk ditindaklanjuti, terutama jika tampaknya terdapat lonjakan prevalensi. Kebanyakan vendor menyimpan daftar email untuk menerima laporan atau sampel tersebut untuk dianalisis dan ditindaklanjuti.

Instalasi perangkat lunak yang tidak terkontrol pada perangkat komputasi dapat menyebabkan timbulnya kerentanan. Organisasi sebaiknya mendefinisikan dan menerapkan kebijakan yang ketat terhadap jenis perangkat lunak yang dapat diinstal oleh pengguna. *Patch* perangkat lunak sebaiknya diterapkan jika dapat membantu menghilangkan atau mengurangi kerentanan keamanan.

Perangkat lunak yang disediakan vendor yang digunakan dalam sistem operasional melalui Internet sebaiknya dipelihara pada level yang didukung oleh pemasok. Seiring waktu, vendor perangkat lunak berhenti mendukung perangkat lunak versi lama. Organisasi sebaiknya mempertimbangkan risiko mengandalkan perangkat lunak yang tidak didukung termasuk perangkat lunak *open source* ketika digunakan dalam sistem operasional. Perangkat lunak sumber terbuka yang digunakan dalam sistem operasional sebaiknya dipelihara hingga rilis perangkat lunak terbaru yang sesuai.

Mitigasi lain untuk kerentanan meliputi:
a) mengubah praktik operasional;
b) mengonfigurasi ulang sistem teknis;
c) menghindari risiko dengan mengelola akses Internet;
d) melakukan pelatihan terhadap staf dan pengguna;
e) menerapkan langkah-langkah pertahanan yang mendalam, yaitu ketika kontrol gagal, ada metode independen lain yang diterapkan untuk terus mempertahankan;
f) menguji keamanan sistem, mengamankan SDLC serta menguji *patch* dan pembaruan sebelum penerapan.

ISO/IEC 27002, ISO/IEC 30111 dan ISO/IEC 29147 memberikan panduan lebih lanjut terkait manajemen kerentanan.

9.2.11 Manajemen jaringan

Mengurangi eksposur aset yang terhubung ke Internet dapat mengurangi risiko terkait akses tidak sah, gangguan, atau kerusakan. Kontrol sebaiknya diimplementasikan untuk menjamin keamanan informasi yang terhubung ke Internet dan pada proteksi dari layanan yang terhubung dari akses yang tidak sah. Kontrol sebaiknya ditetapkan untuk menjaga kerahasiaan dan integritas data yang melewati Internet serta untuk memproteksi sistem dan aplikasi yang terhubung. Sistem yang dapat dihubungkan ke Internet sebaiknya dibatasi dan ketika diizinkan, sebaiknya diautentikasi. Pencatatan dan pemonitoran perangkat dan sistem jaringan yang terkait dengan infrastruktur Internet organisasi, sebaiknya diaplikasikan untuk mencatat dan mendeteksi tindakan yang dapat mempengaruhi, atau relevan dengan, keamanan Internet. Organisasi sebaiknya mempertimbangkan pengelolaan keamanan sistem yang terhubung ke Internet dengan memisahkannya dari jaringan organisasi lain seperti jaringan pribadi dan DMZ. Perimeter jaringan terpisah ini sebaiknya didefinisikan dengan baik dan dikontrol menggunakan *gateway* (misalnya *firewall*, *router* pemfilteran).

Hal-hal berikut sebaiknya dipertimbangkan untuk implementasi keamanan jaringan:
— Memastikan terdapat antarmuka yang termonitor dan reliabel antara jaringan organisasi dan Internet, yang juga memastikan kontrol akses semua entitas, dan bukan hanya orang yang berwenang. Informasi dan aplikasi juga sebaiknya dikontrol sebelum memberikan akses ke dan dari infrastruktur internal.
— Menyusun jaringan internal untuk mengisolasi aset yang sangat kritikal dari aset penggunaan umum, dengan membuat semacam *silos* atau *cluster* dengan kontrol akses yang memadai. Pastikan subjaringan dengan *router* pemfilteran dan subjaringan tertanam untuk menghindari jalur langsung ke aset kritikal.
— Memonitor dan menganalisis trafik internal untuk mendeteksi dan memblokir aktivitas terlarang.
— Memastikan akses dan penggunaan Internet dan layanannya (termasuk komunikasi dengan personel yang bekerja di luar fasilitas fisik) tetap terjaga.
— Memastikan bahwa jaringan internal cukup terpisah dengan proteksi pembatas internal untuk mengisolasi komponen kritikal atau krusial dari titik masuk dan saluran transfer internal yang mudah diakses.

Peraturan mengenai penggunaan Internet dan layanan yang diakses melalui Internet sebaiknya dirumuskan untuk setidaknya mencakup aspek-aspek berikut:
a) layanan jaringan melalui Internet yang dapat diakses oleh pengguna dan prosedur otorisasi untuk layanan tersebut;
b) manajemen jaringan dan kontrol teknologi serta prosedur untuk memproteksi akses terhadap koneksi Internet dan layanan jaringan melalui Internet;
c) sarana yang digunakan untuk mengakses Internet dan layanan melalui Internet (misalnya HTTPS, VPN);
d) pemonitoran layanan yang diakses melalui Internet (misalnya pemantauan lebar pita (*bandwidth*), SIEM).

Firewall adalah perangkat perimeter jaringan kritikal dan organisasi sebaiknya mempertimbangkan teknologi *firewall* yang dapat mengatasi serangan berbasis Internet dengan lebih baik. Tujuan dari perangkat ini adalah untuk memberikan proteksi dari ancaman yang datang dari Internet dan mencegah transfer informasi hak milik yang tidak terkendali ke Internet. Teknologi *router* dapat diterapkan dengan fitur bawaan atau modul tambahan untuk meningkatkan keamanan jaringan dan dapat mengatasi risiko siber seperti serangan DoS dan DDoS.

IDS berbasis jaringan dan teknologi IPS berbasis jaringan dapat diterapkan dengan kecerdasan artifisial dan pembelajaran mesin (*machine learning*) untuk menangani serangan berbasis Internet tingkat lanjut termasuk serangan dengan pola dan perilaku khusus yang diketahui. Bergantung pada pengaturan jaringannya, organisasi dapat mempertimbangkan peralatan jaringan yang dilengkapi dengan berbagai modul keamanan jaringan bawaan seperti *firewall*, IPS, DLP, dan proteksi dari serangan yang menargetkan DNS.

ISO/IEC 27002 dan seri ISO/IEC 27033 memberikan panduan lebih lanjut tentang keamanan jaringan.

9.2.12 Proteksi terhadap perangkat perusak

Perangkat lunak anti-perangkat perusak memindai data dan program untuk mengidentifikasi pola mencurigakan yang terkait dengan perangkat perusak. Untuk memungkinkan deteksi kode berbahaya baru, sangat penting untuk memastikan bahwa perangkat lunak pemindaian selalu diperbarui, sebaiknya melalui pembaruan harian.

Mengingat potensi perangkat perusak baru yang menargetkan kerentanan *zero-day*, terdapat perangkat lunak yang dapat mengidentifikasi varian yang diketahui. Ini termasuk teknologi yang dapat mengidentifikasi pola serangan potensial. Meskipun bukan bukti yang mudah, perangkat lunak ini memberikan level proteksi yang lebih tinggi daripada tidak menggunakannya. Beberapa sistem operasi populer memiliki beberapa fitur bawaan untuk memproteksi dari perangkat perusak umum namun tetap sebaiknya dilengkapi dengan teknologi anti-perangkat perusak untuk lingkungan dengan risiko lebih tinggi.

Implementasi anti-perangkat perusak sebaiknya diperluas ke proteksi dari trafik dan pertukaran Internet yang tidak diinginkan (di kedua arah), karena pengguna umumnya menerima dan mengirim perangkat perusak tanpa menyadarinya. Tindakan pencegahan, deteksi, koreksi dan pemulihan untuk memproteksi dari perangkat perusak sebaiknya diimplementasikan, dikombinasikan dengan kesadaran pengguna yang tepat.

Panduan berikut sebaiknya dipertimbangkan oleh organisasi:

a) menggunakan perangkat lunak anti-perangkat perusak pada gerbang jaringan (*gateway*) ke Internet, untuk memindai semua trafik ke dan dari Internet, termasuk semua protokol jaringan yang diizinkan untuk digunakan;
b) menggunakan perangkat lunak anti-perangkat perusak pada semua sistem klien, khususnya yang digunakan untuk akses Internet oleh pegawai;
c) memindai fail, surel, lampiran pesan instan, halaman web, dan tautan eksternal untuk mencari virus, *ransomware*, *trojan*, dan bentuk perangkat perusak lainnya;
d) memblokir tampilan (*pop-up*) yang mencurigakan, iklan web, situs web berbahaya yang diketahui atau dicurigai, dan menggunakan daftar blokir untuk layanan yang tidak sah, misalnya saluran obrolan atau layanan surel web;
e) menimbulkan kesadaran pengguna bahwa ada risiko lebih besar terkait perangkat perusak ketika berhubungan dengan pihak eksternal melalui tautan eksternal;
f) memverifikasi bahwa informasi akurat terkait perangkat perusak berasal dari sumber yang bermutu dan memiliki reputasi baik (misalnya situs Internet tepercaya atau pemasok perangkat lunak anti-perangkat perusak);
g) mengimplementasikan pencatatan dan pemonitoran untuk semua layanan yang memungkinkan kemungkinan transfer data ke Internet;
h) membatasi penggunaan layanan tidak sah yang memungkinkan transfer data dalam jumlah besar;
i) menerapkan filter untuk protokol tidak resmi, misalnya. protokol jaringan *peer-to-peer*;
j) menambal (*patching*) kerentanan sistem yang diketahui dalam jangka waktu berdasarkan kekritisan kerentanan, dengan fokus pada semua sistem yang menerima trafik Internet;

k) mengonfigurasi sistem dan aplikasi yang diakses melalui Internet, untuk menonaktifkan fungsi yang tidak diperlukan (misalnya makro);
l) menyiapkan perencanaan pemulihan yang tepat dari serangan perangkat perusak, termasuk semua cadangan data dan perangkat lunak yang diperlukan (termasuk cadangan daring dan luring) dan pengaturan pemulihan.

ISO/IEC 27002 memberikan panduan lebih lanjut tentang proteksi terhadap perangkat perusak.

9.2.13 Manajemen perubahan

Kebijakan dan proses manajemen perubahan sebaiknya ditetapkan untuk memastikan bahwa organisasi lebih mudah menerapkan perubahan pada infrastruktur TI, mengelola perubahan pada sistem dan aplikasi TI untuk mencegah gangguan tak terjadwal, kerusakan atau kehilangan data. Organisasi sebaiknya menyertakan perubahan terkait keamanan Internet untuk sistem yang dibawakan di Internet dalam proses manajemen perubahannya. Proses-proses ini membantu organisasi untuk meminta, memprioritaskan, mengotorisasi, menyetujui, menjadwalkan, dan mengimplementasikan setiap perubahan. Kebijakan manajemen perubahan mencakup pernyataan tentang tanggung jawab dan tugas manajer sistem, mengimpor perangkat lunak dan fail, kontrol akses, di antara yang lain. Semua perubahan (modifikasi, perpindahan, penghapusan atau penambahan) komponen atau struktur jaringan sebaiknya dikelola untuk menjaga arsitektur dan gambar infrastruktur tetap mutakhir.

ISO/IEC 27002 memberikan panduan lebih lanjut tentang manajemen perubahan.

9.2.14 Identifikasi undang-undang yang berlaku dan persyaratan kepatuhan

Internet semakin banyak digunakan sebagai platform untuk menyebarkan banyak layanan transaksi daring. Mungkin terdapat undang-undang dan regulasi keamanan data, keamanan siber, dan privasi mengenai proteksi konfidensialitas, integritas, dan ketersediaan detail transaksi.

Transaksi perbankan, saluran pembayaran, transaksi berbasis aplikasi seluler, dan aktivitas perdagangan elektronik lainnya biasanya diatur karena keterlibatan uang dalam bentuk digital. Semua persyaratan hukum, undang-undang, regulasi dan kontrak terkait keamanan informasi dan keamanan siber serta pendekatan organisasi untuk memenuhi persyaratan ini sebaiknya diidentifikasi, didokumentasikan, dan selalu diperbarui.

Diharapkan catatan yang dipelihara pada sistem daring yang diakses melalui Internet terproteksi dari kehilangan, kehancuran, pemalsuan, akses tidak sah, dan rilis tidak sah, sesuai dengan persyaratan hukum, undang-undang, regulasi, kontrak, dan bisnis. Catatan dapat disyaratkan sebagai bukti bahwa suatu organisasi beroperasi sesuai dengan peraturan perundang-undangan, untuk menjamin pertahanan terhadap potensi tindakan perdata atau pidana atau untuk mengonfirmasi status finansial suatu organisasi kepada pihak yang berkepentingan.

ISO/IEC 27002 memberikan panduan lebih lanjut tentang peraturan perundang-undangan dan persyaratan kepatuhan.

9.2.15 Penggunaan kriptografi

Kriptografi adalah salah satu cara untuk memastikan proteksi informasi yang dikirimkan dan mencegah analisis trafik. Jaringan pribadi virtual (*virtual private network*-VPN) adalah solusi sederhana. Kriptografi memiliki beberapa kendala terkait dengan manajemen pengodean dan

penguraian kunci, serta manajemen perangkat kriptografi, yang sebaiknya dianggap konfidensial dan kritikal.

Kriptografi sebaiknya digunakan untuk memproteksi konfidensialitas, autentisitas, dan/atau integritas informasi yang dikirimkan melalui Internet. Implementasi VPN dan HTTPS (*hypertext transfer protocol secure*) menggunakan kriptografi untuk koneksi yang aman. Algoritma, panjang kunci, dan praktik penggunaan kriptografi sebaiknya dipilih berdasarkan praktik terbaik. Manajemen kunci yang tepat membutuhkan proses yang aman untuk menghasilkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan, dan menghancurkan kunci kriptografi.

Semua kunci kriptografi sebaiknya diproteksi dari modifikasi dan kehilangan. Selain itu, kunci rahasia dan privat memerlukan proteksi terhadap penggunaan yang tidak sah, serta pengungkapan. Peralatan yang digunakan untuk menghasilkan, menyimpan, dan mengarsipkan kunci sebaiknya diproteksi secara fisik di mana relevan. Saat menggunakan kriptografi, perlu diingat bahwa regulasi yang berbeda dan batasan nasional dapat berlaku untuk penggunaan teknik kriptografi dan masalah aliran informasi terenkripsi lintas batas.

ISO/IEC 27002 memberikan panduan lebih lanjut tentang penggunaan kriptografi.

9.2.16 Keamanan aplikasi untuk aplikasi hadap-Internet

Teknologi baru dapat diadopsi untuk sistem yang merupakan bagian dari infrastruktur Internet. Teknologi baru sebaiknya dianalisis risiko keamanannya dan desainnya sebaiknya ditinjau terhadap pola serangan yang diketahui. Keamanan sebaiknya ditanamkan saat mendesain sistem. Sistem tersebut juga sebaiknya ditinjau secara berkala untuk memastikan bahwa sistem tersebut tetap mutakhir dalam melawan potensi ancaman baru dan tetap dapat diterapkan terhadap kemajuan teknologi dan solusi yang diterapkan.

Organisasi sebaiknya mengadopsi prinsip rekayasa yang aman termasuk mengimplementasikan siklus hidup pengembangan yang aman untuk mengidentifikasi dan memitigasi risiko dalam produk dan solusi yang sedang dikembangkan. Hal ini sebaiknya mempertimbangkan pemodelan ancaman, teknik autentikasi pengguna, komponen rantai pasokan, kontrol sesi yang aman dan validasi data, sanitasi, dan tinjauan desain yang berorientasi keamanan untuk membantu mengidentifikasi kerentanan keamanan pada sistem hadap-Internet. Kode aplikasi untuk aplikasi hadap-Internet paling baik didesain dari perspektif keamanan berdasarkan asumsi bahwa kode tersebut selalu rentan terhadap serangan, baik melalui kesalahan atau peristiwa yang merusak.

Organisasi sebaiknya menetapkan aturan untuk penggunaan sumber daya melalui Internet yang aman dan tepat, termasuk setiap pembatasan terhadap situs web dan aplikasi berbasis web yang tidak diinginkan atau tidak tepat, dan menginformasikan kepada personel sebagaimana mestinya. Hal ini membuat personel enggan mencoba mengakses situs tersebut. Aturan sebaiknya selalu diperbarui. Situs web tersebut dapat berisi informasi ilegal, virus, dan materi *phishing*. Salah satu teknik untuk membatasi website yang tidak diinginkan atau tidak tepat adalah dengan memblokir alamat IP atau domain website yang bersangkutan. Beberapa pemindai dan teknologi anti-perangkat perusak dapat melakukan hal ini secara otomatis atau dapat dikonfigurasi untuk melakukannya.

Standar pengodean yang aman sebaiknya diikuti untuk mendesain dan mengembangkan aplikasi. Jika pemilik aplikasi dapat mengakses skrip dengan akses jarak jauh langsung ke server, maka penyerang pada prinsipnya juga bisa. Server web sebaiknya dikonfigurasi untuk mencegah penelusuran direktori dalam kasus seperti itu. Pedoman OWASP [23, 24] dapat menjadi referensi yang berguna untuk mengamankan desain dan pengujian aplikasi.

Organisasi sebaiknya mendokumentasikan perilaku kode (*code behaviour*) dan membuat asesmen apakah perilaku tersebut dapat termasuk dalam area potensial yang dapat dianggap sebagai *spyware* atau perangkat lunak yang menipu. Dalam kasus terakhir, organisasi sebaiknya melibatkan asesor yang berkualifikasi untuk mengevaluasi apakah kode tersebut termasuk dalam kriteria objektif vendor anti-*spyware* yang mematuhi praktik terbaik. Hal ini dapat memastikan bahwa perangkat lunak yang disediakan oleh organisasi untuk pengguna akhir tidak akan diberi label sebagai *spyware* oleh vendor anti-*spyware*. Banyak vendor anti-*spyware* memublikasikan kriteria yang mereka gunakan untuk menilai perangkat lunak.

Organisasi sebaiknya mengimplementasikan penandatanganan kode digital pada binernya sehingga vendor anti-perangkat perusak dan anti-perangkat pengintai dapat dengan mudah menentukan pemilik fail. Perangkat lunak yang secara konsisten diproduksi oleh ISV menggunakan praktik terbaik termasuk penandatanganan kode digital, dapat dikategorikan sebagai perangkat lunak yang kemungkinan besar aman. Jika suatu organisasi menemukan teknik perangkat lunak berguna yang dapat membantu mengurangi masalah perangkat pengintai atau perangkat perusak, organisasi tersebut sebaiknya mempertimbangkan untuk bermitra dan bekerja sama dengan vendor agar teknik tersebut tersedia secara luas.

Untuk aplikasi yang transaksinya diproses melalui Internet, hal berikut sebaiknya dipertimbangkan:
— persyaratan level proteksi yang disyaratkan untuk menjaga konfidensialitas dan integritas detail transaksi;
— mentransmisikan detail transaksi melalui Internet dengan kontrol keamanan yang memadai (misalnya jalur transmisi terenkripsi, sertifikasi digital);
— menyimpan detail transaksi di luar lingkungan yang dapat diakses publik dan memastikan media penyimpanan tidak dapat diakses langsung dari Internet;
— persyaratan resiliensi terhadap serangan, yang dapat mencakup persyaratan untuk memproteksi server aplikasi yang terlibat atau memastikan ketersediaan interkoneksi jaringan yang disyaratkan untuk memberikan layanan;
— jika terdapat kebutuhan akan tingkat ketergantungan yang tinggi terhadap keamanan produk perangkat lunak, produk tersebut sebaiknya divalidasi secara independen berdasarkan skema Common Criteria, sebagaimana dideskripsikan dalam seri ISO/IEC 15408.

Pengujian keamanan sebaiknya menjadi bagian integral dari pengujian sistem atau komponen sebelum terekspos ke Internet. Organisasi dapat memanfaatkan alat otomatis, seperti alat analisis kode dan pemindai kerentanan, dan sebaiknya memverifikasi remediasi cacat terkait keamanan sebelum membuat sistem tersebut aktif di Internet.

Pengujian keamanan sebaiknya mencakup pengujian:
a) fungsi keamanan, misalnya autentikasi pengguna, pembatasan akses, penggunaan API yang aman dan penggunaan kriptografi;
b) konfigurasi yang aman termasuk sistem operasi, *firewall* dan komponen keamanan lainnya

Seri ISO/IEC 15408 memberikan panduan tentang jaminan aplikasi. ISO/IEC 27002 dan seri ISO/IEC 27034 memberikan panduan terkait keamanan aplikasi.

9.2.17 Manajemen perangkat titik akhir

Informasi yang disimpan, diproses oleh, atau dapat diakses melalui perangkat titik akhir (misalnya perangkat IoT, perangkat USB, BYOD) sebaiknya diproteksi. Membawa dan menggunakan perangkat titik akhir di area aman sebaiknya dikontrol dengan tepat. Strategi keamanan untuk manajemen perangkat titik akhir sebaiknya dikembangkan dan diimplementasikan. Strategi ini sebaiknya mencakup pengelolaan *firewall* perangkat, alat filter

khusus surel, keamanan dan pemfilteran Internet, pengelolaan dan alat keamanan perangkat seluler, alat enkripsi dan deteksi intrusi.

Keamanan titik akhir menjadi semakin penting, karena titik akhir bergerak keluar dari batas organisasi dan pengguna dapat menggunakan Internet untuk mengakses *cloud* dan sumber daya dalam jaringan organisasi. Pembobolan pada titik akhir sebaiknya ditanggapi dengan tindakan segera untuk memblokir penyerang dan membatasi kerusakan lebih lanjut. Organisasi sebaiknya menerapkan kapabilitas teknis di titik akhir untuk mendeteksi trafik buruk dari sumber yang tidak diketahui dan pelaku jahat, dan menanggapinya. Teknologi seperti itu juga dikenal sebagai teknologi deteksi dan respons titik akhir (EDR). Organisasi sebaiknya memiliki mekanisme untuk memastikan bahwa semua kebijakan keamanan organisasi yang berlaku pada sistem dan perangkat pengguna akhir diaktifkan setiap saat. Teknologi tersebut sebaiknya memastikan bahwa pengguna akhir tidak dapat menonaktifkan atau melewati fitur keamanan yang diinstal pada titik akhir mereka.

Hilangnya atau terbobolnya titik akhir dapat menjadi risiko yang signifikan terhadap data yang berada di titik akhir termasuk perangkat seluler. Organisasi sebaiknya menerapkan teknik untuk memastikan bahwa mereka dapat melacak perangkat tersebut dan jika perangkat tersebut hilang atau dibobol, mereka sebaiknya dapat menghapus konten perangkat dari jarak jauh bahkan sebelum datanya dicuri oleh pelaku kejahatan.

ISO/IEC 27002 memberikan panduan lebih lanjut tentang manajemen perangkat titik akhir (*endpoint*).

9.2.18 Pemonitoran

Log yang mencatat aktivitas, pengecualian, kesalahan, dan kejadian relevan lainnya sebaiknya dibuat, diproteksi, disimpan, dan dianalisis. Log sebaiknya diproteksi dan disimpan di lokasi yang aman untuk analisis dan audit log. Beberapa regulasi mensyaratkan penyimpanan log untuk jangka waktu tertentu. Jaringan, sistem, dan aplikasi hadap-Internet sebaiknya dimonitor terhadap perilaku anomali dan tindakan yang tepat sebaiknya diambil untuk mengevaluasi potensi insiden keamanan informasi.

ISO/IEC 27002 memberikan panduan lebih lanjut tentang pemonitoran.

Lampiran A
(informatif)
Rujukan silang antara dokumen ini dan ISO/IEC 27002

Tabel A.1 menunjukkan korespondensi antara kontrol keamanan Internet yang disebutkan dalam 9.2 dokumen ini dan kontrol yang terdapat dalam ISO/IEC 27002. Setiap kolom berisi nomor subpasal dan subjudul yang relevan.

Tabel A.1 — Pemetaan antarkontrol untuk keamanan Internet

ISO/IEC 27032	**ISO/IEC 27002:2022**
9.2.2 Kebijakan keamanan Internet	5.1 Kebijakan keamanan informasi 5.4 Tanggung jawab manajemen
9.2.3 Kontrol akses	5.15 Kontrol akses 5.16 Manajemen identitas 5.18 Hak akses 8.2 Hak akses privilese 8.18 Penggunaan program utilitas privilese
9.2.4 Edukasi, kesadaran, dan pelatihan	6.3 Kesadaran, edukasi, dan pelatihan keamanan informasi
9.2.5 Manajemen insiden keamanan	5.7 Intelijen ancaman 5.24 Perencanaan dan persiapan manajemen insiden keamanan informasi 5.25 Asesmen dan keputusan tentang peristiwa keamanan informasi 5.26 Respons terhadap insiden keamanan informasi 5.27 Belajar dari insiden keamanan informasi 5.28 Pengumpulan bukti 6.8 Pelaporan peristiwa keamanan informasi
9.2.6 Manajemen aset	5.9 Inventori informasi dan aset terkait lainnya 5.10 Penggunaan yang akseptabel dari informasi dan aset terkait lainnya 5.11 Pengembalian aset 5.12 Klasifikasi informasi
9.2.7 Manajemen pemasok	5.19 Keamanan informasi dalam hubungan pemasok 5.20 Menangani keamanan informasi dalam perjanjian pemasok 5.21 Memanajemeni keamanan informasi dalam rantai pasokan TIK 5.22 Memonitor, reviu, dan manajemen perubahan layanan pemasok 5.23 Keamanan informasi untuk penggunaan layanan *cloud*
9.2.8 Keberlangsungan bisnis melalui Internet	5.29 Keamanan informasi selama disrupsi 5.30 Kesiapan TIK untuk kontinuitas bisnis

	8.13 Pencadangan informasi 8.14 Redundansi fasilitas pemrosesan informasi
9.2.9 Proteksi privasi melalui Internet	5.34 Privasi dan proteksi PII 8.11 Penyembunyian data (*data masking*)
9.2.10 Manajemen kerentanan	8.8 Manajemen kerentanan teknis 8.9 Manajemen konfigurasi 8.19 Instalasi perangkat lunak pada sistem operasional
9.2.11 Manajemen jaringan	8.16 Memonitor aktivitas 8.20 Keamanan jaringan 8.21 Keamanan layanan jaringan 8.22 Segregasi jaringan
9.2.12 Proteksi terhadap perangkat perusak	8.7 Proteksi terhadap perangkat lunak perusak
9.2.13 Manajemen perubahan	8.32 Manajemen perubahan
9.2.14 Identifikasi undang-undang yang berlaku dan persyaratan kepatuhan	5.28 Pengumpulan bukti 5.31 Persyaratan legal, statutori, regulatori, dan kontraktual 5.33 Proteksi rekaman
9.2.15 Penggunaan kriptografi	8.24 Penggunaan kriptografi
9.2.16 Keamanan aplikasi untuk aplikasi hadap-Internet	8.23 Pemfilteran web 8.24 Penggunaan kriptografi 8.25 Siklus hidup pengembangan yang aman 8.26 Persyaratan keamanan aplikasi 8.27 Prinsip arsitektur dan rekayasa sistem yang aman 8.28 Pengodean yang aman 8.29 Pengujian keamanan dalam pengembangan dan penerimaan
9.2.17 Manajemen perangkat titik akhir	8.1 Perangkat titik akhir pengguna 8.9 Manajemen konfigurasi
9.2.18 Pemonitoran	8.15 Membuat log 8.16 Memonitor aktivitas

Bibliografi

[1] ISO 9000:2015, Quality management systems — Fundamentals and vocabulary

[2] ISO/IEC 15408 (all parts)

[3] ISO 19101-1:2014, Geographic information — Reference model — Part 1: Fundamentals

[4] ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements

[5] ISO/IEC/TR 23187:2020, Information technology — Cloud computing — Interacting with cloud service partners (CSNs)

[6] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems — Requirements

[7] ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls

[8] ISO/IEC 27005:2022, Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[9] ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

[10] ISO/IEC 27018:2019, Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

[11] ISO/IEC 27031:2011, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[12] ISO/IEC 27033 (all parts), Information technology — Security techniques — Network security

[13] ISO/IEC 27034 (all parts), Information technology — Application security

[14] ISO/IEC 27035 (all parts), Information technology — Security techniques — Information security incident management

[15] ISO/IEC 27036 (all parts), Cybersecurity — Supplier relationships

[16] ISO/IEC/TS 27100:2020, Information technology — Cybersecurity — Overview and concepts

[17] ISO/IEC 27701:2019, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines

[18] ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework

[19] ISO/IEC 29146:2016, Information technology — Security techniques — A framework for access management

[20] ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure

[21] ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes

[22] ISO 31000:2018, Risk management — Guidelines

[23] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Web Security Testing Guide, [online] [viewed 2020-12-03]. Available at https://owasp.org/www-project-web-security-testing-guide/

[24] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top 10, [online] [viewed 2022-10-29]. Available at https://owasp.org/Top10/

Cybersecurity — Guidelines for Internet security

1 Scope

This document provides:

— an explanation of the relationship between Internet security, web security, network security and cybersecurity;

— an overview of Internet security;

— identification of interested parties and a description of their roles in Internet security;

— high-level guidance for addressing common Internet security issues.

This document is intended for organizations that use the Internet.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
attack vector
path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome

EXAMPLE 1 IoT devices.

EXAMPLE 2 Smart phones.

3.2
attacker
person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

[SOURCE: ISO/IEC 27033-1:2015, 3.3]

3.3
blended attack
attack that seeks to maximize the severity of damage and speed of contagion by combining multiple attack vectors (3.1)

3.4
bot
automated software program used to carry out specific tasks

Note 1 to entry: This word is often used to describe programs, usually run on a server, that automate tasks such as forwarding or sorting e-mail.

Note 2 to entry: A bot is also described as a program that operates as an agent for a user or another program or simulates a human activity. On the Internet, the most ubiquitous bots are the programs, also called spiders or crawlers, which access websites and gather their content for search engine indexes.

3.5
botnet
collection of remotely controlled malicious bots that run autonomously or automatically on compromised computers

EXAMPLE: Distributed denial-of-service (DDoS) nodes, where the botnet controller can direct the user's computer to generate traffic to a third-party site as part of a coordinated DDoS attack.

3.6
cybersecurity
safeguarding of people, society, organizations and nations from cyber risks

Note 1 to entry: Safeguarding means to keep cyber risk at a tolerable level.

[SOURCE: ISO/IEC TS 27100:2020, 3.2]

3.7
dark net
network of secret websites within the Internet that can only be accessed with specific software

Note 1 to entry: The dark net is also known as the dark web.

3.8
deceptive software
software which performs activities on a user's computer without first notifying the user as to exactly what the software will do on the computer, or asking the user for consent to these actions

EXAMPLE 1 A program that hijacks user configurations.

EXAMPLE 2 A program that causes endless popup advertisements which cannot be easily stopped by the user.

EXAMPLE 3 Adware and spyware.

3.9
hacking
intentionally accessing a computer system without the authorization of the user or the owner

3.10
hacktivism
hacking (3.9) for a politically or socially motivated purpose

3.11
Internet
global system of inter-connected networks in the public domain

[SOURCE: ISO/IEC 27033-1:2015, 3.14, modified — “the” has been deleted from the term.]

3.12
Internet security
preservation of confidentiality, integrity and availability of information over the Internet (3.11)

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

Note 2 to entry: Please refer to definitions on confidentiality, integrity, availability, authenticity, accountability, non-repudiation and reliability in ISO/IEC 27000:2018, Clause 3.

3.13
Internet service provider
ISP
organization that provides Internet services to a user and enables its customers access to the Internet (3.11)

Note 1 to entry: Also, sometimes referred to as an Internet access provider (IAP).

3.14
malicious content
applications, documents, files, data or other resources that have malicious features or capabilities embedded, disguised or hidden in them

3.15
malware
malicious software
software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to the user and/or the user’s computer system

EXAMPLE Viruses, worms and trojans.

3.16
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: In the context of this document, an individual is distinct from an organization.

Note 2 to entry: In general, a government is also an organization. In the context of this document, governments can be considered separately from other organizations for clarity.

[SOURCE: ISO 9000:2015, 3.2.1, modified — Note 1 to entry and Note 2 to entry have been replaced.]

3.17
phishing
fraudulent process of attempting to acquire private or confidential information by masquerading as a trustworthy entity in an electronic communication

Note 1 to entry: Phishing can be accomplished by using social engineering or technical deception.

3.18
potentially unwanted software
deceptive software (3.8), including malicious (3.15) and non-malicious software, that exhibit the characteristics of deceptive software

3.19
spam
unsolicited emails that can carry malicious content and/or scam messages

Note 1 to entry: While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, wiki spam, mobile phone messaging spam, Internet forum spam and junk fax transmissions.

[SOURCE: ISO/IEC 27033-1:2015, 3.37, modified — Note 1 to entry has been added.]

3.20
spyware
deceptive software (3.8), that collects private or confidential information from a computer user
Note 1 to entry: Information can include matters such as websites most frequently visited or more sensitive information such as passwords.

3.21
threat
potential cause of an unwanted incident, which can result in harm to a system, individual or organization (3.16)

3.22
trojan
malware (3.15) that appears to perform a desirable function for the user but that mislead the user of its true intent

3.23
vishing
voice phishing done to acquire private or confidential information by masquerading as a trustworthy entity

Note 1 to entry: Vishing can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.

3.24
waterhole technique
technique inciting people to access a website that specifically contains (lots of) malware

Note 1 to entry: Waterhole is also known as watering hole.

3.25
World Wide Web
Web
universe of network-accessible information and services

[SOURCE: ISO 19101-1:2014, 4.1.40]

4 Abbreviated terms

The following abbreviated terms are used in this document.

AI	artificial intelligence
API	application programming interface
APT	advanced persistent threat
BYOD	bring your own device
CERT	computer emergency response team
DDoS	distributed denial-of-service
DLP	data loss prevention
DMZ	demilitarized zone
DNS	domain name system
DoS	denial-of-service
EDR	endpoint detection and response
FTP	file transfer protocol
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol over secure socket layer
ICANN	Internet corporation for assigned names and numbers
ICT	information and communications technology
IDS	intrusion detection system
IETF	Internet engineering task force
IMT	incident management team
IoT	Internet of things
IP	Internet protocol
IPS	intrusion prevention system
ISP	Internet service provider
ISV	independent software vendor
IRT	incident response team
ISMS	information security management system
OWASP	open web application security project
PII	personally identifiable information
SDLC	software development life cycle
SIEM	security information and event management
SME	small and medium enterprises
URL	uniform resource locator
USB	universal serial bus
VPN	virtual private network
W3C	World Wide Web consortium
WWW	World Wide Web

5 Relationship between Internet security, web security, network security and cyber security

Figure 1 shows a high-level view of the relationship between Internet security, web security, network security and cybersecurity.

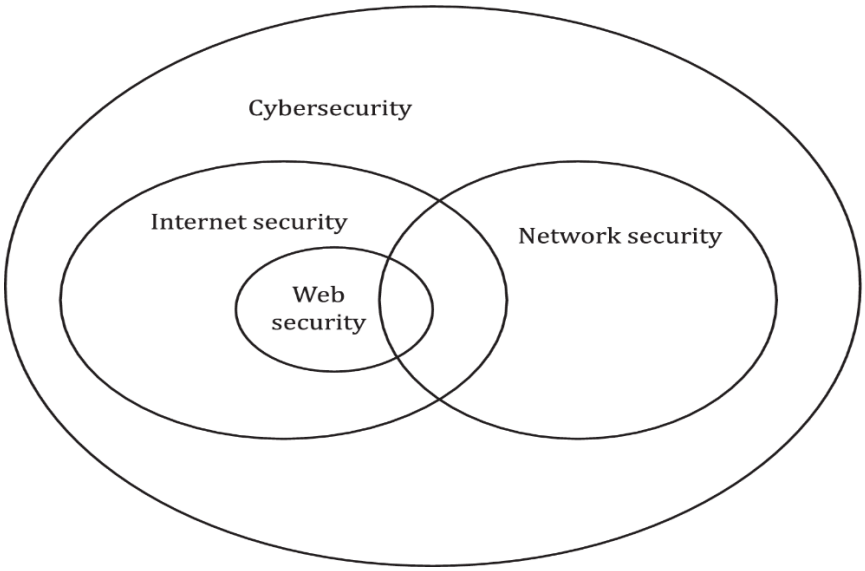


Figure 1 — Relationship between Internet security, web security, network security and cybersecurity

The Internet is a global system of inter-connected digital networks in the public domain. The information exchange on the Internet also uses the mobile telephony network that is hence part of the Internet. This global network connects billions of servers, computers, and other hardware devices. Each device is connected with any other device through its connection to the Internet. The Internet creates an environment which is conducive to information sharing.

Internet security is concerned with protecting Internet-related services and related ICT systems and networks as an extension of network security. These efforts aim to reduce Internet related security risks for organizations, customers and other relevant stakeholders.

Internet security also ensures the availability and reliability of Internet services. Over the Internet, various services are on offer, such as file transfer services, mail services or any services that can be publicly shared with the end users. In this context, Internet security deals with the secure delivery of these services over the public network.

The web is one of the ways information is shared on the Internet [others include email, file transfer protocol (FTP), and instant messaging services]. The web is composed of billions of connected digital documents that can be viewed using a web browser. A website is a set of related web pages that are prepared and maintained as a collection in support of a single purpose.

Web security deals with information security in the context of World Wide Web (WWW) and with web services accessed over the public network. The web service is enabled by the use of HTTP protocol in which any registered publicly available URL can be accessed. Web security also deals with security of this HTTP connection used for information exchange.

A network can include components such as routers, hubs, cabling, telecommunications controllers, key distribution centres, and technical control devices. Network security broadly

covers all kinds of networks that exist within an organization from local area network, wide area network, personal area network and wireless networks.

Network security is concerned with the design, implementation, operation and improvement of networks, as well as the identification and treatment of network-related security risks within organizations, between organizations, and between organizations and users.

Cybersecurity concerns managing information security risks when information is in digital form in computers, storage and networks. Many of the information security controls, methods, and techniques can be applied to manage cyber risks.

Cybersecurity also deals with protecting Internet-connected systems including hardware, software, programs and data from potential attacks. Many of these attacks are characterized by targeted and blended attacks with a high degree of sophistication and persistence. The threats can be Internet-based and/or threats due to connectivity with other networks and systems within the organization or customer and service provider’s network, to which the organization communicates during the normal course of business.

6 Overview of Internet security

The personally identifiable information (PII) of Internet users is captured by many sites and services offered on the Internet. This includes application service providers who closely track user activities and use artificial intelligence (AI) techniques to provide recommendations for purchases, healthcare, time management and a host of other feedback intending to make their lives and tasks easier to manage. Many of these sites collect this data without the users’ permission and provide this data to other third parties for monetary gain, again without the users' knowledge. Interested parties have been establishing their presence on the Internet through websites, conducting e-Commerce on a global scale, providing digital services on the Internet, using public cloud services to deliver services and using web-based business applications and services.

Many uses of the Internet involve exchange of information and provision of services that do not concern people and PII. PII varies by jurisdiction. The security of such information and services can be critical to interested parties. Furthermore, the range of hardware connected to the Internet as either individual devices or private networks is increasing rapidly in the so-called Internet of things. Autonomy and application of artificial intelligence within the Internet of things creates challenging Internet security requirements.

While the Internet can facilitate significant business outcomes, there are always many security risks to be managed. It is important to remember that the Internet was not originally designed with security features in mind. Organizations rely heavily on the use of the Internet to conduct their business. Owing to a low level of trust associated with the Internet, business operations can face significant adverse consequences from the loss of confidentiality, integrity, and availability of information and services, if not adequately controlled.

While some individuals are careful in managing their online identity, most people upload details of their personal profiles to share with others. Profiles on many sites, in particular social networking sites and chat rooms, can be downloaded and stored by other parties. This can lead to the creation of a digital dossier of personal data that can be misused, disclosed to other parties, or used for secondary data collection. While the accuracy and integrity of this data are questionable, they create links to individuals and organizations that often cannot be completely erased. These developments in the communication, entertainment, transportation, shopping, financial, insurance, and healthcare domains create new risks to interested parties on the Internet. Thus, risks can be associated with loss of privacy over the Internet.

The convergence of information and communication technologies, the ease of getting into the Internet from desktops, laptops to mobile and IoT devices, and the narrowing of personal space between individuals, are gaining the attention of malicious actors and criminal organizations.

These entities are using mechanisms such as phishing, spam and spyware, as well as developing attack techniques like zero-day attacks, vishing, malicious websites and other deception techniques to exploit any weaknesses they can discover on the Internet.
In recent years, security attacks on the Internet have evolved from hacking for personal fame to organized crime or cybercrime. A plethora of tools and processes previously observed in isolated cybersecurity incidents are now being used together in multi-blended attacks, often with far reaching malicious objectives.

Many of these tools are also available on public software repositories and other publicly available resources. The objectives of an attack range from personal attacks, identity theft, financial frauds or thefts, to hacktivism and information manipulation on the Internet. Much of the stolen personal data and customer data are also made available on the dark net, which can be publicly accessible. Organizations, and SMEs in particular, should understand the real consequences of “manipulating” information on the Internet. These security risks are the cyber risks to the users accessing the Internet.

As the Internet is a global public network, transactions can originate from any part of the world, as can attacks. The multiple modes of business transactions that are carried out on the Internet are becoming the target of cybercrime syndicates. Ranging from business-to-business, business-to-consumer to consumer-to consumer services, the risks posed are inherently complex.

Another complexity arises from the fact that all interested parties, even when they are not malicious, have a different view on their needs, requirements and threats, hence they have a different list of risks and controls to counter them. This means that there is no “one size fits all” solution.

Criteria such as what constitutes a transaction or an agreement are dependent on the specific legal and regulatory environments across jurisdictions. These criteria also depend on the interpretation of the law and how each party in the relationship manages their liability. Often, the issue of using data collected during the transaction or relationship is not addressed adequately. This can eventually lead to security concerns such as the leakage of information.

The legal and technical challenges posed by these Internet issues are far-reaching and global in nature. The challenges can only be addressed through collaboration between the information security technical community, legal community and different regions to adopt a coherent strategy. This strategy should take into account the role of each interested party and existing initiatives, within a framework of international cooperation.

Information travels through the Internet instantly, meaning that attacks can also happen instantly. As these speeds are not easily apprehended by human mind, the attack is always discovered a long time after it occurred, and damages are already potentially huge. In most cases, the identity of the attackers is hidden. Therefore, the use of artificial intelligence (AI) is frequently proposed to counter the attacks.

7 Interested parties

7.1 General

Interested parties of Internet security include those who:
— use services over the Internet;
— use the Internet to provide services;
— provide the infrastructure and communicating capabilities of the Internet;
— globally coordinate the operation of the Internet;
— provide and enforce laws and regulations.

The interested parties of Internet security can be categorized as users (7.2), coordinators and standardization organizations (7.3), government authorities (7.4), law enforcement agencies (7.5) and Internet service providers (7.6).

7.2 Users

Users is a term that refers to individuals, end-users as well as private and public organizations using the Internet. Private organizations include small and medium enterprises (SMEs), as well as large enterprises. Government and other public agencies are collectively referred to as public organizations. An individual or an organization becomes a user when they access the Internet or any services available over the Internet. Users can make use of Internet services, view or collect information. They can also provide certain specific information which is within an application's space, or open to limited members or groups within the application's space, or the general public.

User roles can include, but are not limited to, the following:
— general Internet application user, or general user, such as online game player, instant messenger user, or web surfer;
— buyer/seller, involved in placing goods and services on online auction and marketplace sites for interested buyers, and vice versa;
— blogger and other contents contributor (for example, an author of an article on a wiki), in which information in text and multimedia (for example, video clips) are published for general public or limited audience's consumption;
— member of an organization (such as an employee of a company, or other form of association with a company);
— other roles, whereby a user can be assigned a role unintentionally or without their consent.

EXAMPLE 1 When a user visits a site which requires authorization, and intentionally or unintentionally gains access, the user can be labelled as an intruder.

EXAMPLE 2 An individual, acting as buyer or seller, can unknowingly participate in criminal transactions of selling stolen goods or money laundering activities.

Organizations often use the Internet to publicize company and related information, as well as market related products and services. Organizations also utilize the Internet as part of their network for delivery and receipt of electronic messages (for example, emails) and other documents (for example, file transfer).

In line with the same principles of being a good corporate citizen, these organizations should extend their corporate responsibilities to the Internet by proactively ensuring that their practices and actions in the Internet usage do not introduce further security risks into the Internet user community.

Some proactive measures include:
— information security management by implementing and operating an effective information security management system (ISMS) (see ISO/IEC 27001 for requirements for information security management systems);
— implementing controls based on ISO/IEC 27002 and other relevant standards, without operating an ISMS;
— security monitoring and incident response;
— incorporating security as part of the software development life-cycle (SDLC), where the level of security built into systems should be determined based on the organization's criticality of data;
— regular security education of users in the organization through continuous technology and process updates and keeping track of latest technology developments; and
— understanding and using proper channels in communicating with vendors and service providers on security issues discovered during usage.

7.3 Coordinator and standardization organisations

Coordinator and standardization organisations (ICANN, IETF, W3C etc.) develop technical standards on the use of the Internet and the services provided by the service providers. They advise organizations of their roles and responsibilities on the Internet.

7.4 Government authorities

Governments hold information on national security, strategic, military, intelligence issues among many other elements relating to the government and state, but also a vast array of information on individuals, organizations and society as a whole.

Governments should protect their own country's infrastructure and information from unauthorized access and exploitation. There is a growing and expanding trend of offering e-government services using the Internet. This is a new channel, among others, to launch attacks and access the abovementioned information which, if successful, can result in serious impact to a region, its government and society.

Government authorities play a coordination role between law enforcement agencies and are the primary coordinator for disseminating information and orchestrating any required resources, both at national-level and corporate level, in times of crisis arising from a massive cyber-attack. This also includes authorities like CERT and similar organizations that are entrusted with such responsibilities depending on the specific region in context.

Governments mandate cybersecurity education programmes for universities and high schools, and ensure that an appropriate public-private-partnership is organized with the necessary legal structure, that organizes the law enforcement agencies and defines their missions.

7.5 Law enforcement agencies

Law enforcement agencies enforce the regulations and hold all interested parties accountable in terms of their compliance to the relevant regulations within its national jurisdiction.

7.6 Internet service providers

Service providing organizations can include two categories:
— providers of access to the Internet for employees and partners;
— providers of services to consumers of the Internet.

These services are provided either to a closed community (for example, registered users), or the general public, through the delivery of applications including cloud-service providers over the Internet. A consumer can also be a service provider, if it in turn provides a service over the Internet or enables another consumer to access the Internet.

Service providers can also be understood as carriers or wholesalers, versus distributors and retailers of access services. This distinction is important from a security and, especially, law enforcement perspective. In the event that a distributor or retailer is unable to provide adequate security or lawful access, support services often default back to the carrier or wholesaler. Internet service providers (ISPs) can provide support by supervising the “traffic” and providing alternative routes or hosts for traffic control. They also can look for "dangerous" transfers over the Internet. With the necessary legal authorizations and those of the users, they can filter what is dangerous, as it is the case with solutions providing “sand boxes” to verify transferred files for malware. ISPs can warn their customers when they discover threat patterns.

8 Internet security risk assessment and treatment

8.1 General

ISO 31000 provides principles and generic guidelines on risk management while ISO/IEC 27005 provides guidelines and processes for information security risk management in an organization, supporting the requirements of an ISMS according to ISO/IEC 27001. The guidelines and processes provided by these documents are recommended for addressing risk management in the context of the Internet. It is the responsibility of the interested parties to define their approach for risk management. Several existing methodologies can be used under the framework described in ISO/IEC 27005 to conduct a risk assessment and manage the risks associated with the organization’s use of the Internet, considering the relevant threats and vulnerabilities and the Internet security issues.

In organizations where there are limited resources available, the controls are required to take into account the rationality between the organizational needs for security and resources to avoid errors in the selection of controls. An inappropriate selection of controls may result in additional risks or ineffective controls.

8.2 Threats

A threat agent is an individual or group of individuals who have any role in the execution or support of an attack. Thorough understanding of their motives (religious, political, economic, etc.), capabilities (knowledge, funding, size, etc.) and intentions (fun, crime, espionage, etc.) is critical in the assessment of vulnerabilities and risks, as well as in the development and deployment of controls.

Malware can result in the compromise of security controls (e.g. capture and disclosure of passwords), unintended disclosure of information, unintended changes to information, destruction of information, and/or unauthorized use of system resources. Malware is commonly delivered through viruses, worms, and trojans with far-reaching consequences.

A virus is an executable and replicable program that inserts its own code into legitimate programs with the objective of damaging the host computer (i.e. deleting files and programs, corrupting storage and operating systems). In its simplest state, a worm is a computer program meant to self-replicate and spread to other computers through outbound messages to all the addresses in a user's contact list to drain a system’s resources. Additionally, just like a virus, a worm can propagate code that can damage its host. Such code is referred to as a payload (e.g. the ability to encrypt files in ransomware and the installation of system backdoors that

enable remote access). A trojan is a malicious program disguised as or embedded within legitimate software that has similar objectives to viruses and worms, but, unlike either of them, does not replicate or propagate on its own.

Internet security threats to personally identifiable information (PII) of Internet users revolve mainly around identity issues, posed by the leakage or theft of personal information. If a person's online identity is stolen or masqueraded, the person can be deprived of access to key services and applications. In more serious scenarios, the consequences can range from financial to national level incidents. Unauthorized access to a person's financial information also opens up the possibility of theft of the person's money and fraud.

EXAMPLE 1 Credit information can be sold on the black market or darknet, which can facilitate online identity theft.

EXAMPLE 2 Other examples of threats that in turn equate to threats to life include cyber bullying, online stalking and exploitation crimes including child exploitation and human trafficking.

Another threat is the possibility of the endpoint including personal devices and bring your own device (BYOD) being made a zombie or a bot. Computing devices can become compromised and thereby part of a larger botnet. The online presence and online business of an organization are often targeted by miscreants whose intent is more than plain mischief.

On a larger scale, the infrastructure that supports the Internet can be targeted as well. While this does not affect the functioning of the Internet permanently, it affects the reliability and availability of the infrastructure, which contributes to the security of the Internet.
On a national or international level, the Internet is an area in which illegal behaviour in a given jurisdiction thrives. Due to the nature of the Internet, specifically the challenges in defining boundaries and borders, it is difficult to regulate and control the way that it can be used.

Criminals can either legitimately buy the applications, services and resources that facilitate their cause, or they can resort to illegal means of securing these resources to avoid detection and tracking. This can include acquiring massive computing resources through botnets.

Another threat relates to the deliberate modification of publicly available or proprietary information, or creation of fake information and hoaxes that, if relied upon, can generate serious damage.

8.3 Vulnerabilities

Vulnerability is weaknesses of an asset or control that can be exploited by a threat. Manufacturers, software developers and other technology developers produce security updates and patches to fix these weaknesses once they are found and solved. As systems receive patches, updates or new elements are added. As systems become outdated or unsupported by the vendor or not patched to the latest version, new vulnerabilities can be introduced. Interested parties should have a thorough knowledge and understanding of the asset or control in question, as well as the threats, threat agents and risks involved, in order to perform a comprehensive assessment. Interested parties should be aware of the zero-day vulnerabilities for which there is no patch available.

Web applications accessed over the Internet are susceptible to a variety of vulnerabilities that are introduced by poor design, poorly written code and poorly built production libraries and executables. Examples of such vulnerabilities include the authentication bypass, database injection attacks and cross-site scripting attacks. In these attacks, requests can be manipulated to abuse the webserver functionality.

8.4 Attack vectors

Attack vector is a path or means by which an attacker can gain access to a computer or network server in order to deliver a malicious outcome.

Port scanners are one of the oldest and still very effective tools used by attackers. They scan all ports available on the Internet-facing system to confirm which ports are open. This normally is one of the first steps executed by a prospective attacker on the target Internet-facing system. While the initial attack always targets a publicly facing system (e.g. router, server, firewall, website, etc.), attackers can also seek to exploit assets residing inside the private network that are connected to these publicly facing systems.

Listening to communication channels is a simple and easy attack vector. It is also one of the oldest. Copying and analysing the traffic can be extremely valuable for detecting entry points and initiate other threat vectors. An attacker can also use communication hijacking (by tailgating or piggy-backing) and disguise themselves behind the identity or credentials, and at the expense of the legitimate user without them knowing.

Many of the attacks on the Internet are carried out using malicious software, such as spyware, worms and viruses. Information is often gathered through phishing techniques. An attack can occur as a singular attack vector or carried out as a blended attack or a targeted attack. These attacks can be propagated via, for example, suspicious websites, unverified downloads, spam emails, remote exploitation, zero-day exploitation, and infected removable media.

Other mechanisms growing in use and sophistication, for carrying out attacks, are those based on social networking websites and the use of corrupted files on legitimate websites. Legitimate websites can also be hacked into and have some of their files corrupted and used as a means for perpetrating attacks. Individuals tend to implicitly trust commonly visited websites. Attackers can apply the waterhole technique to compromise a specific group of end users by infecting frequently visited websites. Besides the attacks launched by human attackers, malware infected computers also launch various attacks to surrounding connected computers.

With the proliferation of peer-to-peer applications, commonly used to share files such as digital music, video, photos, etc., attackers are becoming increasingly sophisticated in how to disguise themselves and their malicious code using the exchanged files as a Trojan for their attacks. Once an attacker, through identity theft, can disguise themselves as a legitimate contact, the attacker can engage others, and a new avenue is open for launching the various types of attacks.

Another technique is IP spoofing, in which the attacker manipulates the IP address associated with their messages in an attempt to disguise it as a known, trusted source, thus gaining unauthorized access to systems.

The attacker does not always use the same attack vector. It uses multiple vectors and changes them frequently. Some attacks are hidden to such an extent that they are not detected until it is already too late for the user. Defenders should consider this and look for defence against multiple vectors and not only those already used against them.

IoT devices, smart phones, etc. can be connected to the Internet. These devices can act as an additional attack vector just like any other Internet-connected device, if they are not adequately controlled when connected to the organization’s network.

An advanced persistent threat (APT) is a method of attack with a goal of stealing information over a long period of time whereby attackers gain ongoing access to an organization’s network, establish themselves undetected, move laterally, look, learn and remain in the network.

Another old attack method is brute force. This uses trial and error to guess login credentials, encryption keys, finding hidden web pages whereby attackers work through all possible combinations hoping to guess correctly to gain access to an organization's network and information.

9 Security guidelibes for the Internet

9.1 General

Interested parties can assess risks by taking into account threats that apply to their assets. This analysis can aid in the selection of controls to counter the risks and reduce them to an acceptable level. Controls are implemented to reduce the likelihood or consequences of such risks, and to meet security requirements of the interested parties (either directly or indirectly by providing direction to other parties).

Vulnerabilities can remain after the implementation of controls. Such vulnerabilities can be exploited by threat agents. Interested parties seek to minimize the risk, given other constraints. Interested parties should be confident that the controls are adequate to counter the threats to assets before they allow exposure of assets to the specified threats. If the interested parties do not possess the capability to evaluate all aspects of the controls, they can seek evaluation of the controls using external organizations.

An effective way to confront Internet security risks involves a combination of multiple strategies, taking into consideration the various interested parties.

These strategies include:
— industry specific approaches, with collaboration of all interested parties to identify and address Internet issues and risks;
— broad consumer and employee education, providing a trusted resource for how to identify and address specific Internet risks within the organization as well as in the community of Internet users;
— innovative technology solutions to help protect consumers from known Internet-based attacks, to stay current and be prepared against new exploitations;
— updated legislation and regulations to enable justice to prevail across jurisdictions.

9.2 Controls for Internet security

9.2.1 General

Most organizations use the Internet for various purposes, from web surfing, blogging, social networking and accessing public cloud services, to information sharing and doing e-commerce business. This involves sharing of classified business information including personal information while executing online transactions. The Internet being a public network is prone to certain unique threats. If not addressed, these threats result in attacks that can be difficult to manage.

Organizations should develop policies, procedures and response capability to:
a) define the rules for acceptable use of the Internet by personnel;
b) define what services may be exposed over the Internet;
c) identify the threats, vulnerabilities, attack vectors and their associated risks;
d) define the roles and responsibilities of various users of the Internet;
e) conduct user awareness on the safe practices for Internet usage;

f) specify the responsible departments for handling Internet security issues;
g) establish a response mechanism for cybersecurity incidents;
h) conduct security drills to test the response mechanism towards attacks originating from the Internet.

Based on risk assessment, one can uncover the various relevant Internet security risks that can be addressed through various controls as explained below.

9.2.2 Policies for Internet security

An organization should prepare and publish a policy concerning Internet usage by personnel and other relevant parties in alignment with security objectives. This determines which Internet services are used, who is authorized to use them, and what the security objectives are. This policy directs all other guidelines for the secure connection to, and use of, the Internet.

Policies for Internet security should be defined, approved by management, published and communicated to, and acknowledged by, the relevant personnel, contractors and external parties. The Internet security policies should stipulate the personnel authorized to access the Internet, the content they can view, prohibited conduct on the Internet, among others. Responsibilities should be allocated for all activities pertaining to the Internet, and for the design, approval, implementation, operation and monitoring of all the specific controls applicable to Internet security.

ISO/IEC 27002 provides further guidance on policies for Internet security.

9.2.3 Access control

Access control includes access rights not only for users, but also other entities such as devices, applications or automated processes. Therefore, every connection should be authenticated, and every activity duly authorized, based on the roles and permissions established according to the business and security rules, and each entity should be assigned the least privileged permissions. This enhances the traceability of access to information and assets, and reduces anonymity to increase security.

Rules to control physical and logical access to information and assets, other assets associated with the Internet and information processing facilities should be established and implemented based on business and information value. Rules regarding access to essential information and assets, other assets associated with information and information processing facilities should be in line with an established access control policy and information classification policy.

Accounts should only be restricted to users who are authorized due to their job role or function. Each user should have separate accounts and they should not be shared, nor should the same password be used for more than one account.

Access rights to information, systems, applications and services should be provisioned, reviewed, adjusted, modified and removed according to the organization’s policy and procedure on access control. The allocation and use of privileged access rights should be restricted and controlled. Secure authentication technologies and procedures should be implemented based on information access restrictions and related access control rules. Password management systems should be put in place to manage and support the process of password creation and the quality thereof.

Information systems directly connected to the Internet (e.g. firewall infrastructure, network perimeter devices, etc.) can have one or more privileged utility programs that can be capable of overriding system and application controls. If an attacker gets access to any of the systems,

then these privileged utility programs, if not properly controlled, can result in privileged access by the attacker.
These programs should be adequately controlled by the organization so that intruders do not get access to such privileged utility programs and override system and application controls. Effective access management should include:
— regular review of all access rights;
— regular review of administrative logs.

ISO/IEC 27002 and ISO/IEC 29146 provide further guidance on access management.

9.2.4 Education, awareness and training

Organization's personnel (including top management, system admin, IT staff and privileged users etc.) should be regularly updated on the main threats (e.g. phishing and vishing) and the actions to be taken to prevent them and respond in case of improper action.

Numerous new threats are launched on the Internet daily and are continuously evolving and becoming more stealthy and sophisticated. When implementing a control to counter an attack, it is possible users are not aware that they are the victim of an attack that is new or more sophisticated.

Organizations should provide regular awareness and training material for personnel using a variety of formats such as email communications, online training and messaging through intranets, to inform personnel of online threats as well as their obligations of acceptable use and reporting incidents. This provides a level of understanding and catches their attention to protect both themselves and the organization.

ISO/IEC 27002 provides further guidance on education, awareness and training.

9.2.5 Security incident management

Security incidents on the Internet can range from a wide variety of cyber-attacks on Internet-facing organizational resources, as well as servers, databases and applications that are behind the Internet facing resources. Security incidents can be triggered from anywhere on the Internet. Sometimes the host that is carrying the attack can be a compromised host. Some incidents can be sophisticated in nature and involve special skills to adequately respond. Incidents often cross national, geographical and organizational boundaries, and the speed of information flow and changes from the unfolding incident often gives limited time for the responding individuals and organizations to act.

An incident management team (IMT) with a supporting incident response team (IRT) should be established to provide the organization with capability for assessing, responding to and learning from such incidents. Incident response procedures should consider detecting and reporting the occurrence of security events like potential and actual incidents by human or automatic means. Monitoring tools implemented by the organization can detect and send security events for incident response. Threat intelligence is information about threats and threat actors that helps mitigate harmful events in cyberspace. Information security personnel should continuously scan threat intelligence sources like social media intelligence, human intelligence, technical intelligence or intelligence from the deep and dark web, collect the information and then analyse it.

A technical solution to support information sharing and coordination should be established to help prepare and respond to security events and cyber incidents. This is an important step that organizations should take as part of their security controls. Such a solution should involve information sharing and coordination that should be secure, effective, reliable and efficient.

Incidents pertaining to Internet security should be responded to by a nominated contact and other relevant persons of the organization or interested parties. Any external requirements on reporting of incidents to relevant interested parties within the defined time frame (e.g. incident notification requirements to regulators within defined time frames) should be considered when implementing incident management procedures. The organization should establish and maintain contact with the relevant legal, regulatory, and supervisory authorities. The organizations should also maintain contact with special interest groups and other specialist security forums and professional associations.

There is a need for efficient and effective information sharing, coordination and incident handling among interested parties in Internet security. This collaboration should be in a secure and reliable manner that also protects the privacy of individuals concerned. Many of the interested parties can reside in different geographical locations and time zones and are likely to be governed by different regulatory requirements.

Information sharing and collaboration includes:
— key elements of considerations for establishing trust;
— necessary processes for collaboration and information exchange and sharing;
— technical requirements for systems integration and interoperability between different interested parties.

The organization using the Internet should define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence in case of a security incident. It is expected that evidence is collected in a manner that is admissible in the appropriate national courts of law or international authorities in case the incident is proved to have originated from another country as per the monitoring logs and other digital evidence.

Digital evidence can transcend organizational or jurisdictional boundaries in case of a security incident. In such cases, it should be ensured that the organization is entitled to collect the required information as digital evidence for future course of action. The correct setting of computer clocks is important to ensure the accuracy of audit logs, which can be expected for investigations in case of any attacks from over the Internet or expected as evidence in possible legal action.

The information gained from the evaluation of security incidents of Internet-facing systems should be used to identify recurring or related incidents in order to plan and implement changes to reduce the likelihood or impact of future similar incidents. Tools like IPS and SIEM can be re-configured based on the evaluation of the security incidents and relevant policy amendments can be initiated to prevent future incidents.
ISO/IEC 27002 and the ISO/IEC 27035 series provide further guidance on incident management.

9.2.6 Aset management

ICT components containing critical information and applications should be identified. Traditionally, organizations have been expected to know where their assets are physically located in order to protect them adequately. Organizations should not only keep an inventory of up-to-date ICT assets within their control but should also maintain an information asset register of where their information is processed, stored, transferred, whether it is on their internal network or uses cloud/Internet-based hosting solutions. In this manner, the organization can manage the risks to their information wherever it resides and make risk-based decisions regarding whether it is appropriate for that information to be stored outside the organization's control environment. Similarly, for network components, organizations are expected to know where the sensitive assets are located with regards to the entry points for

potential attackers. This can be the official Internet access — via the firewall — and all the other connections with devices, (e.g. smartphones, IoT). Organizations should also identify critical paths used to access sensitive ICT assets or to transport sensitive information within the organization's network. These paths should not be visible, accessible or monitorable by intruders. Without this knowledge, no adequate segregation of networks is possible. This inventory should take the form of network architecture (location of the functionalities) and infrastructure, both clearly indicating the entry/connection points with the Internet (all the interconnected networks).

Rules for the acceptable use and procedures for the handling of assets, other assets associated with the Internet and related processing facilities should be identified, documented and implemented. Organizations should have and use a procedure to evaluate the criticality of information and ICT assets that hold and transfer them. This would allow the organization to clearly identify what should be protected and at what level in terms of generic policies and network security.

ISO/IEC 27002 provides further guidance on asset management.

9.2.7 Supplier management

Processes and procedures should be identified and implemented to manage the Internet security risks associated with the use of suppliers. All relevant information security requirements should be established and agreed with each supplier based on the type of supplier and associated risks. Risk management in relation with the ICT suppliers and the information they store, exploit or can have access to, is key for preparing contracts that ensure that the organization's information security objectives are continuously achieved.

Agreement with suppliers relevant to the Internet (like ISPs and cloud service providers over the Internet) should be established and documented to ensure that there is a clear understanding between the organization and the suppliers regarding both parties' obligations to fulfil relevant information security requirements. Organizations should have open partnerships with the ISPs, telecommunication service providers, cloud service providers and partners to inform/warn of detections of incoming threats. The ability of the Internet service provider to manage agreed services in a secure way should be determined and regularly monitored. It is expected that the organization and the service provider reach an agreement on the right to audit.

For cloud services accessible over the Internet and as subscribed by the organization, the organization is expected to review and negotiate the cloud service agreements with the cloud service provider(s). The organization should undertake the relevant risk assessment to identify the risks associated with using the cloud services and manage the risks for the duration of the agreement. It is expected that the cloud service agreement addresses the confidentiality, integrity, availability and PII handling requirements of the organization. For any cloud services where an organization is unable to negotiate the terms of the agreement, it is expected that the organization enters the agreement with eyes wide open, understanding the risks of using the service and how to manage these risks for the duration of the agreement.

Cloud-based tools like web meeting tools, web chatting tools and cloud storage tools pose the risk to an organization if these tools have inherent security bugs that can be exploited by bad actors, therefore it is important for the organization to establish security controls for usage of these cloud-based tools.

The following can be considered for inclusion in the agreements in order to satisfy the identified Internet security requirements:

a) legal and regulatory requirements, including information protection requirements at the ISP's end like protection from DDoS and other attacks;
b) obligation of each contractual party to implement an agreed set of controls including access control, network and system monitoring, reporting and auditing; as well as the supplier’s obligations to comply with the organization’s security requirements;
c) incident management requirements and procedures (especially notification and collaboration during incident remediation);
d) monitoring, review and change management of supplier services to ensure that the information security terms and conditions of the agreements are being adhered to, and that they allow the monitoring of service performance levels to verify adherence to the agreements, monitor changes made by suppliers and monitor changes in supplier services.

ISO/IEC 27002, the ISO/IEC 27036 series, ISO/IEC TR 23187 and ISO/IEC 27017 provide further guidance related to suppliers.

9.2.8 Business continuity over the Internet

Some business activities like Internet based trading and other e-commerce activities depend on the organization’s Internet infrastructure within the organization. Disruptions to Internet services can be caused by DoS and DDoS attacks from bad actors, perimeter device malfunction or any disruption from the ISP end. DoS and DDoS attacks can also be conducted by bad actors on the ISP end that can result in complete outage of the Internet backbone. Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Any disruptions in the Internet infrastructure constitute continuity risks to the organization and should be addressed by the organization. Organizations should plan for procurement of Internet services from different ISPs for basic continuity measures. Organizations should deploy security measures to avoid disruptions like anti-DDoS measures for continuity of network devices. Organizations can also require respective ISPs to deploy anti-DDoS measures within the ISP network. Regardless of the continuity service, organizations should continue to consider information security in any solution even when in business continuity mode.

ISO/IEC 27002, ISO 22301 and ISO/IEC 27031 provide further guidance related to ICT continuity.

9.2.9 Privacy protection over the Internet

Most service providers control or process PII. When this information is used for purposes different to the interests of the data principal, privacy concerns are raised. A hosting service provider processes PII on their network and data centre as part of their business services. These services, which include websites and other online applications, are often re-packaged and resold by hosting subscribers to other consumers, such as small businesses and end-users and made accessible over the Internet.

Should the hosting subscribers set up an insecure server, or host malicious contents in their sites or applications, the security of the consumers including PII stored by such online applications, will be adversely affected. As such, it is important that services, at a minimum, meet best practice standards by complying with the minimum terms of agreements that covers the privacy requirements of the users. In addition to the data protection and personal privacy provisions on the Internet-facing site or application, service providers should require such sites or applications hosted on their networks to implement a set of best practice security controls at the application level before they go live. Prior to signing up to a service on the Internet,

organizations should undertake a privacy impact assessment (PIA) to identify the personal information that can be used, collected, processed, stored or transmitted and the associated privacy risks to determine whether they are acceptable to the organization and manage these accordingly. This does not only include collecting customer data to provide a service but can also include collecting metadata such as IP addresses or geolocation data of individuals browsing websites. Organizations should publish a privacy notice on their site to clearly inform all their users of the requirements of interacting with the organization's online services. Data masking should be used according to the organization's policy on access control and business requirements, taking legal requirements into consideration. DLP measures should be applied to systems and networks that process, store or transmit sensitive information. There are technological features in some Internet browsers, that allow privacy settings to be changed by the user.

ISO/IEC 27002, ISO/IEC 27701, ISO/IEC 29100 and ISO/IEC 27018 provide further guidance related to privacy.

9.2.10 Vulnerability management

Information about vulnerabilities of ICT systems being used should be obtained in a timely fashion. The organization's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken to address the associated risk. Configurations, including security configurations of hardware, software, services and networks should be established, documented, implemented, and monitored and reviewed.

Organizations that supply technology products (firewall, IDS, IPS etc.) and services (network services, VoIP services, managed security services etc.) should consistently and effectively implement measures to identify, handle and disclose vulnerabilities of the products and services they supply. Based on the vulnerabilities disclosed by the product and service vendors, appropriate protection measures are implemented to address the vulnerabilities.

With the increasing proliferation of malware on the Internet, a service providing organization can receive reports relating to malware and spyware infections and other security issues. Such information is important and useful for relevant vendors to assess the risk of malware infection, and provide updates to necessary tools to ensure that any new malware or spyware detected can be removed or disabled effectively. In this regard, an organization should establish contact with security vendors and submit relevant reports and malware samples to the vendors for follow-up, particularly if there appears to be a spike in prevalence. Most vendors maintain an email list for receiving such reports or samples for analysis and follow-up.

Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities. The organization should define and enforce strict policy on which types of software users can install. Software patches should be applied when they can help to remove or reduce security vulnerabilities.

Vendor supplied software used in operational systems over the Internet should be maintained at a level supported by the supplier. Over time, software vendors cease to support older versions of software. The organization should consider the risks of relying on unsupported software including open-source software when used in operational systems. Open-source software used in operational systems should be maintained to the latest appropriate release of the software.

Other mitigations for vulnerabilities include:
a) changing the operational practices;
b) reconfiguring the technical systems;
c) avoiding the risk by managing Internet access;

d) training staff and users;
e) applying defence in-depth measures i.e. where one controls fails, there is another independent method in place to continue to defend;
f) system security testing, secure SDLC and testing of patches, updates before deployment.

ISO/IEC 27002, ISO/IEC 30111 and ISO/IEC 29147 provide further guidance related to vulnerability management.

9.2.11 Network management

Reducing the exposure of assets connected to Internet reduces risks related to unauthorized access, tampering or damage. Controls should be implemented to ensure the security of information connected to the Internet and to the protection of connected services from unauthorized access. Controls should be established to safeguard the confidentiality and integrity of data passing over the Internet and to protect the connected systems and applications. Systems that can be connected to the Internet should be restricted and where permitted, should be authenticated. Logging and monitoring of network devices and systems associated with the organization's Internet infrastructure, should be applied for recording and detecting actions that can affect, or are relevant to, Internet security. The organization should consider managing the security of systems connected to the Internet by segregating the same from other organizational networks like private networks and DMZ. The perimeter of this segregated network should be well defined and should be controlled using a gateway (e.g. firewall, filtering router).

The following should be considered for network security implementation:
— Ensure there is a monitored and reliable interface between the organization’s network and the Internet, that also ensures access control of all entities, and not only authorized people. Information and applications should also be controlled before granting both access to and from the internal infrastructure.
— Structure the internal network to isolate highly critical assets from general use assets, by creating kind of silos or clusters with adequate access control. Ensure sub-networks with filtering routers and imbedded sub-networks to avoid having a straight path to critical assets.
— Monitor and analyse internal traffic to detect and block illicit activities.
— Ensure the access and use of Internet and its services (including the communication with personnel working outside the physical facilities) is preserved.
— Ensure that the internal network is sufficiently segregated with internal border protections to isolate critical or crucial components from the entry-points and easy to access internal transfer channels.

Rules should be formulated on the use of Internet and services accessed over the Internet to cover the following aspects at a minimum:
a) the network services over the Internet that may be accessed by the user and authorization procedures for such services;
b) network management and technological controls and procedures to protect access to Internet connections and network services over the Internet;
c) the means used to access Internet and services over the Internet (e.g. HTTPS, VPN);
d) monitoring of the services accessed over the Internet (e.g. bandwidth monitoring, SIEM).

A firewall is a critical network perimeter device and organizations should consider firewall technologies that can better address the Internet-based attacks. The aim of this device is to provide a protection from the threats coming from the Internet and prevent the uncontrolled transfer of proprietary information to the Internet. Router technologies can be deployed with in-built features or add-on modules to enhance network security and can address cyber risks like DoS and DDoS attacks.

Network-based IDS and network-based IPS technologies can be deployed with artificial intelligence and machine learning to deal with advanced Internet-based attacks including attacks with known signature patterns and behaviour. Depending upon their network setup, organizations can consider network appliances that come with in-built various network security modules like firewall, IPS, DLP and protection from attacks targeting DNS.

ISO/IEC 27002 and the ISO/IEC 27033 series provide further guidance on network security.

9.2.12 Protection against malware

Anti-malware software scans data and programs to identify suspicious patterns associated with malware. To enable detection of new malicious code, it is very important to ensure that the scanning software is always kept up to date, desirably through daily updates.

Given the potential for new malware to target zero-day vulnerabilities, software exists that can identify known variants. This includes technology that can identify potential attack patterns. While not fool proof, this software does provide a higher level of protection than not using it. Several popular operating systems have some embedded features to protect against common malware but should still be supplemented with anti-malware technology for higher risk environments.

Anti-malware implementation should be expanded to the protection of unwanted Internet traffic and exchange (in both directions), as users generally receive and send malware without knowing it. Prevention, detection, correction and recovery measures to protect against malware should be implemented, combined with appropriate user awareness.

The following guidance should be considered by the organization:

a) using anti-malware software on the gateways to the Internet, for scanning all traffic to and from the Internet, including all network protocols authorized for use;
b) using anti-malware software on all client systems, especially those used for Internet access by employees;
c) scanning files, emails, instant messaging attachments, webpages and external links for viruses, ransomware, trojans and other forms of malware;
d) blocking suspicious pop-ups, web advertisements, known or suspected malicious websites, and using blocklists for unauthorized services, e.g. chat channels or web mail services;
e) making users aware that there are greater risks associated with malware when dealing with external parties over external links;
f) verifying that accurate information relating to malware comes from qualified and reputable sources (e.g. reliable Internet sites or suppliers of anti-malware software);
g) implementing logging and monitoring for all services which allow the possibility to transfer data towards the Internet;
h) restricting the use of unauthorised services which enable the transfer of big amounts of data;
i) implementing filters for non-authorized protocols, e.g. peer-to-peer networking protocols;
j) patching known system vulnerabilities within time frames based on vulnerability criticality, with focus on all systems receiving Internet traffic;
k) configuring systems and applications accessed over the Internet, to disable functions that are not necessary (e.g. macros);
l) preparing appropriate plans for recovering from malware attacks, including all necessary data and software backup (including both online and offline backup) and recovery arrangements.

ISO/IEC 27002 provides further guidance on protection against malware.

9.2.13 Change management

Change management policies and processes should be established to ensure that it is easier for organizations to roll out changes to the IT infrastructure, manage changes to IT systems and applications in order to prevent unscheduled disruption, data corruption or loss. Organizations should include Internet security related changes for systems hosted on the Internet in its change management process. These processes help the organization to request, prioritize, authorize, approve, schedule and implement any changes. Change management policies include statements on responsibilities and duties of system managers, importing software and files, access control, among others. All changes (modifications, moves, removals or additions) of network components or structure should be managed to keep the architecture and the infrastructure drawings up to date.

ISO/IEC 27002 provides further guidance on change management.

9.2.14 Identification of applicable legislation and compliance requirements

The Internet is increasingly used as a platform to deploy many online transaction services. There can be data security, cybersecurity and privacy laws and regulations on protection of confidentiality, integrity and availability of transaction details.

Banking transactions, payment channels, mobile app-based transactions and other e-commerce activities are usually regulated due to involvement of money in digital form. All information security and cyber security relevant legal, statutory, regulatory and contractual requirements and the organization’s approach to meet these requirements should be identified, documented and kept up to date.

It is expected that records maintained on online systems accessed over the Internet, are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legal, statutory, regulatory, contractual and business requirements. Records can be required as evidence that an organization operates within statutory or regulatory rules, to ensure defence against potential civil or criminal action or to confirm the financial status of an organization to interested parties.

ISO/IEC 27002 provides further guidance on legislation and compliance requirements.

9.2.15 Use of cryptography

Cryptography is one of the ways to ensure the protection of the transmitted information and prevent traffic analysis. A virtual private network (VPN) is a simple solution. Cryptography has some constraints associated with the management of the ciphering and deciphering keys, and the management of the cryptographic devices, which should be considered as confidential and critical.

Cryptography should be used to protect the confidentiality, authenticity and/or integrity of information transmitted over the Internet. Implementation of VPN and HTTPS (hypertext transfer protocol secure) uses cryptography for secure connections. Cryptographic algorithms, key lengths and usage practices should be selected according to best practice. Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use, as well as disclosure. Equipment used to generate, store and archive keys should be physically protected where relevant. When

using cryptography, it should be kept in mind that different regulations and national restrictions can apply to the use of cryptographic techniques and the issues of trans-border flow of encrypted information.

ISO/IEC 27002 provides further guidance on use of cryptography.

9.2.16 Application security for Internet-facing applications

New technology can be adopted for systems that are part of the Internet infrastructure. The new technology should be analysed for security risks and the design should be reviewed against known attack patterns. Security should be embedded while designing the system. The systems should also be regularly reviewed to ensure that they remain up to date in terms of combatting any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

Organizations should adopt secure engineering principles including implementing a secure development life cycle to identify and mitigate risks in products and solutions being developed. This should consider threat modelling, user authentication techniques, supply chain components, secure session control and data validation, sanitization and a security-oriented design review to help identify security vulnerabilities on Internet-facing systems. Application code for Internet-facing applications is best designed from the security perspective based upon the assumption that it is always subject to attack, through either error or malicious events.

Organizations should establish rules for safe and appropriate use of resources over the Internet, including any restriction to undesirable or inappropriate websites and web-based applications, and inform its personnel accordingly. This discourages personnel from trying to access such sites. The rules should be kept up to date. Such websites can contain illegal information, viruses and phishing materials. A technique for restricting an undesirable or inappropriate website is blocking the IP address or domain of the website concerned. Some browser and anti-malware technologies can do this automatically or can be configured to do so.

Secure coding standards should be followed to design and develop applications. If the application owner can access scripts by direct remote access to the server, so can an attacker in principle. Web servers should be configured to prevent directory browsing in such cases. The OWASP guidelines[23, 24] can be a useful reference to secure application design and testing.

Organizations should document code behaviour and make an assessment as to whether the behaviour can fall into potential areas that can be considered as spyware or deceptive software. In the latter case, organizations should engage a suitably qualified assessor to evaluate whether the code falls within anti-spyware vendors objective criteria that adheres to best practices. This can ensure that the software tools provided by organizations for the end-users would not be labelled as spyware by anti-spyware vendors. Many anti-spyware vendors publish the criteria by which they rate software.

Organizations should implement digital code signing for their binaries so that anti-malware and anti-spyware vendors can easily determine the owner of a file. Software consistently produced by ISVs using best practices including digital code signing, can be categorized as likely to be secure. Should an organization discover useful software techniques that can help to reduce the spyware or malware problem, the organization should consider partnering and working with the vendor to make them broadly available.

For applications where the transactions are processed over the Internet, the following should be considered:

— requirements for the level of protection required to maintain the confidentiality and integrity of transaction details;
— transmitting transaction details over the Internet with adequate security controls (e.g. encrypted transmission path, digital certification);
— storing transaction details outside of any publicly accessible environment and ensuring the storage medium is not directly accessible from the Internet;
— resilience requirements against attacks, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections required to deliver the service;
— where there is the need for a high degree of reliance on the security of software products, the products should be independently validated under the Common Criteria scheme, as described in the ISO/IEC 15408 series.

Security testing should be an integral part of the testing for system or components before exposure to the Internet. The organization can leverage automated tools, such as code analysis tools and vulnerability scanners, and should verify the remediation of security related defects before making the systems live on the Internet.

Security testing should include testing of:
a) security functions, e.g. user authentication, access restriction, secure use of APIs and use of cryptography;
b) secure configurations including that of operating systems, firewalls and other security components.

The ISO/IEC 15408 series provides guidance on application assurance. ISO/IEC 27002 and the ISO/IEC 27034 series provide guidance related to application security.

9.2.17 Endpoint device management

Information stored on, processed by or accessible via endpoint devices (e.g. IoT devices, USB devices, BYOD) should be protected. Carrying and using endpoint devices in secure areas should be appropriately controlled. A security strategy for endpoint device management should be developed and implemented. This strategy should include the management of device firewalls, email specific filtering tools, Internet security and filtering, mobile device management and security tools, encryption and intrusion detection tools.

Endpoint security has become even more important, as endpoints are moving outside the organizational perimeter and users may use the Internet to access the cloud and resources within the organization’s network. Compromise at the endpoint should be responded with immediate action to block the attacker and to limit further damage. Organizations should deploy technical capabilities at the endpoints to detect any bad traffic from unknown sources and bad actors, and respond. Such technologies are also known as endpoint detection and response (EDR) technologies. Organizations should have a mechanism to ensure that all the organizational security policies applicable to the end user systems and devices are enabled at all times. Such technologies should make sure that the end user is not able to disable or bypass the security features installed on their endpoint.

Loss or compromise of the endpoint can be a significant risk to the data residing on the endpoint including mobile devices. Organizations should deploy techniques to ensure that they can track these devices and in case of any loss or compromise of the device, they should be able to remotely wipe the contents of the devices even before the data are stolen by the bad actors.

ISO/IEC 27002 provides further guidance on endpoint device management.

9.2.18 Monitoring

Logs that record activities, exceptions, faults and other relevant events should be produced, protected, kept and analysed. Logs should be protected and kept in a secure location for log analysis and audit. Some regulations require storing logs for a certain period of time. Internet-facing networks, systems, and applications should be monitored for anomalous behaviour and appropriate actions should be taken to evaluate potential information security incidents.

ISO/IEC 27002 provides further guidance on monitoring.

Annex A
(informative)
Cross-references between this document and ISO/IEC 27002

Table A.1 shows the correspondence between the controls for Internet security cited in 9.2 of this document and the controls contained in ISO/IEC 27002. Each column contains the relevant subclause number and subheading.

Table A.1 — Mapping between controls for Internet security

ISO/IEC 27032	ISO/IEC 27002:2022
9.2.2 Policies for Internet security	5.1 Policies for information security 5.4 Management responsibilities
9.2.3 Access control	5.15 Access control 5.16 Identity management 5.18 Access rights 8.2 Privileged access rights 8.18 Use of privileged utility programs
9.2.4 Education, awareness and training	6.3 Information security awareness, education and training
9.2.5 Security incident management	5.7 Threat intelligence 5.24 Information security incident management planning and preparation 5.25 Assessment and decision on information security events 5.26 Response to information security incidents 5.27 Learning from information security incidents 5.28 Collection of evidence 6.8 Information security event reporting
9.2.6 Asset management	5.9 Inventory of information and other associated assets 5.10 Acceptable use of information and other associated assets 5.11 Return of assets 5.12 Classification of information
9.2.7 Supplier management	5.19 Information security in supplier relationships 5.20 Addressing information security within supplier agreements 5.21 Managing information security in the ICT supply chain

	5.22 Monitoring, review and change management of supplier services 5.23 Information security for use of cloud services
9.2.8 Business continuity over the Internet	5.29 Information security during disruption 5.30 ICT readiness for business continuity 8.13 Information backup 8.14 Redundancy of information processing facilities
9.2.9 Privacy protection over the Internet	5.34 Privacy and protection of PII 8.11 Data masking
9.2.10 Vulnerability management	8.8 Management of technical vulnerabilities 8.9 Configuration management 8.19 Installation of software on operational systems
9.2.11 Network management	8.16 Monitoring activities 8.20 Networks security 8.21 Security of network services 8.22 Segregation of networks
9.2.12 Protection against malware	8.7 Protection against malware
9.2.13 Change management	8.32 Change management
9.2.14 Identification of applicable legislation and compliance requirements	5.28 Collection of evidence 5.31 Legal, statutory, regulatory and contractual requirements 5.33 Protection of records
9.2.15 Use of cryptography	8.24 Use of cryptography
9.2.16 Application security for Internet-facing applications	8.23 Web filtering 8.24 Use of cryptography 8.25 Secure development life cycle 8.26 Application security requirements 8.27 Secure system architecture and engineering principles 8.28 Secure coding 8.29 Security testing in development and acceptance
9.2.17 Endpoint device management	8.1 User endpoint devices 8.9 Configuration management
9.2.18 Monitoring	8.15 Logging 8.16 Monitoring activities

Bibliography

[1] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[2] ISO/IEC 15408 (all parts)

[3] ISO 19101-1:2014, *Geographic information — Reference model — Part 1: Fundamentals*

[4] ISO 22301:2019, *Security and resilience — Business continuity management systems — Requirements*

[5] ISO/IEC/TR 23187:2020, *Information technology — Cloud computing — Interacting with cloud service partners (CSNs)*

[6] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[7] ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls*

[8] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[9] ISO/IEC 27017:2015, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[10] ISO/IEC 27018:2019, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[11] ISO/IEC 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[12] ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*

[13] ISO/IEC 27034 (all parts), *Information technology — Application security*

[14] ISO/IEC 27035 (all parts), *Information technology — Security techniques — Information security incident management*

[15] ISO/IEC 27036 (all parts), *Cybersecurity — Supplier relationships*

[16] ISO/IEC/TS 27100:2020, *Information technology — Cybersecurity — Overview and concepts*

[17] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[18] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[19] ISO/IEC 29146:2016, *Information technology — Security techniques — A framework for access management*

[20] ISO/IEC 29147:2018, *Information technology — Security techniques — Vulnerability disclosure*

[21] ISO/IEC 30111:2019, *Information technology — Security techniques — Vulnerability handling processes*

[22] ISO 31000:2018, *Risk management — Guidelines*

[23] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Web Security Testing Guide, [online] [viewed 2020-12-03]. Available at https://owasp.org/www-project-web-security-testing-guide/

[24] OPEN WEB APPLICATION SECURITY PROJECT (OWASP). OWASP Top 10, [online] [viewed 2022-10-29]. Available at https://owasp.org/Top10/

Informasi pendukung terkait perumus standar

[1] Komtek perumus SNI
Komite Teknis 35-04 Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi

[2] Susunan keanggotaan Komtek perumus SNI
Ketua : Soetedjo Joewono
Sekretaris : Didik Utomo
Anggota : 1. Bety Hayat Susanti
2. Bisyron Wahyudi
3. Chandra Yulistia
4. Pedro Libratu Putu Wirya
5. Pratama Dahlian Persadha
6. Sarwono Sutikno
7. Satriyo Wibowo
8. Sari Agustini Hafman
9. Sugi Guritman
10. Wisnoe Prasetyo Pribadi
11 . Zaenal Arifin

[3] Konseptor rancangan SNI
Gugus Kerja 4 – Komtek 35-04:
Ketua : Sarwono Sutikno
Wakil Ketua : Pedro Libratu Putu Wirya
Sekretaris : Yasril Andriawan
Anggota : 1. Yusuf Kurniawan
2. Agus Salim
3. Didik Utomo
4. Ricky Aji Pratama
5. Javalina
6. Ruth Novida Sihite

[4] Sekretariat pengelola Komtek perumus SNI
Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara (BSSN)