BUMN Insight

BUMN Insight / Januari 2025 / No. 06

Kementerian BUMN Indonesia prioritaskan keamanan siber

Keputusan Menteri Badan Usaha Milik Negara Nomor SK-275/MBU/11/2024 Tentang Prioritas Penerapan Keamanan Siber di Lingkungan Badan Usaha Milik Negara (BUMN)

Kementerian BUMN telah mengeluarkan **Keputusan Menteri Badan Usaha Milik Negara Nomor SK-275/MBU/11/2024 tentang Prioritas Penerapan Keamanan Siber di Lingkungan Badan Usaha Milik Negara** untuk **melindungi BUMN dari serangan siber yang dapat mengganggu operasi dan menyebabkan kerugian finansial serta reputasi**. Hal ini sejalan dengan ketentuan **Pasal 208 Peraturan Menteri Badan Usaha Milik Negara Nomor PER-02/MBU/03/2023 tentang Pedoman Tata Kelola dan Kegiatan Korporasi Signifikan Badan Usaha Milik Negara**.

Keputusan Menteri ini mewajibkan Perusahaan untuk agar paling sedikit melakukan hal-hal sebagai berikut:

1. **Mengimplementasikan 15 minimum kontrol terkait keamanan siber**
   Implementasi kontrol meliputi proses identifikasi, proteksi, deteksi, respon, dan pemulihan.

Identifikasi - 3 kontrol
Pemeliharaan inventaris seluruh aset serta seluruh akun pengguna dan akun layanan yang dikelola Perusahaan.

Proteksi - 3 kontrol
Pembatasan hak akses administrator, implementasi dan pemeliharaan *Anti-Malware Software*, serta pengelolaan kontrol akses atas aset yang terhubung dari jarak jauh.

Deteksi - 4 kontrol
Pengumpulan, sentralisasi, dan peninjauan *log audit* serta pengelolaan konfigurasi *anti-malware untuk memblokir removable media port secara* otomatis.

Respon - 3 kontrol
Penghapusan/ menonaktifkan akun yang sudah tidak aktif, menentukan personel untuk mengelola penanganan insiden, serta mengelola proses respons insiden.

Pemulihan - 2 kontrol
Pengelolaan *backup* secara otomatis serta melakukan uji coba pemulihan menggunakan backup.

Uraian dan implementasi atas 15 kontrol dimaksud **dibedakan lingkupnya berdasarkan klasifikasi risiko yang telah ditetapkan oleh Kementerian BUMN** yang terdiri dari Sistemik A, Sistemik B dan Netral.

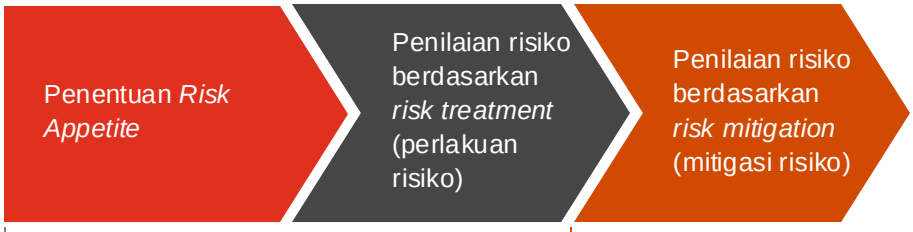
2. Menerapkan kerangka keamanan siber berstandar internasional

Perusahaan BUMN dapat menerapkan kerangka keamanan siber berdasarkan standar internasional seperti CIS, NIST, dan ISO 27001, serta menyesuaikannya dengan prioritas dan kebutuhan masing-masing.

3. Melakukan Penilaian Risiko (*risk assessment*) atas minimum kontrol yang tidak dapat diimplementasikan

Penilaian risiko tersebut mencakup:

Risk treatment adalah langkah-langkah atau strategi yang diimplementasikan oleh Perusahaan untuk mengelola risiko yang telah diidentifikasi dalam rangka mencapai tujuan bisnis atau operasional. Proses ini terdiri dari beberapa tahapan untuk mengurangi, mentransfer, atau mengelola risiko sesuai dengan *risk appetite* Perusahaan tersebut.



Risk appetite adalah selera penerimaan risiko untuk mencapai tujuan perusahaan. *Risk appetite* dapat bervariasi antar BUMN di masing-masing sektor industri dan merupakan bagian dari strategi manajemen risiko secara keseluruhan

Risk mitigation merujuk pada serangkaian tindakan atau strategi yang dirancang untuk mengurangi kemungkinan terjadinya risiko atau mengurangi dampak negatif dari risiko yang terjadi

4. **Menggunakan *tools* pendukung implementasi kontrol**
   Dalam rangka mendukung implementasi kontrol, Perusahaan dapat menggunakan *tools* pendukung, seperti *Security Information & Event Management* (SIEM), *Lightweight Directory Access Protocol* (LDAP), *Privilege Access Management* (PAM), dan lain sebagainya.

5. **Menerapkan prinsip kolaborasi**
   Perusahaan diharapkan menerapkan kontrol terkait keamanan siber dengan kolaborasi antar BUMN maupun dengan Forum Digital BUMN.

6. **Melakukan pelaporan penerapan kontrol secara berkala**
   Perusahaan melaporkan penerapan kontrol terkait keamanan siber secara berkala setiap 1 (satu) tahun sekali pada Laporan Tahunan BUMN.

Pokok utama dari Keputusan Menteri Badan Usaha Milik Negara

Pada era digital yang terus berubah, Keputusan Menteri ini memberi peluang bagi Perusahaan BUMN untuk memperkuat strategi keamanan siber, meningkatkan keunggulan kompetitif, dan memastikan berjalannya perlindungan berkelanjutan dari ancaman siber.

Keputusan ini menyediakan acuan minimum yang perlu diterapkan pada Perusahaan BUMN dan dapat dioptimalkan dengan standar internasional lain nya seperti CIS, NIST, dan ISO 27001.

Beberapa hal untuk meningkatkan keamanan dan ketahanan siber antara lain:

Perencanaan pemulihan bencana dan kelangsungan bisnis

Memiliki strategi yang jelas untuk merespons dan memulihkan dari insiden keamanan siber adalah esensial. Elemen ini mencakup kebijakan dan prosedur untuk memulihkan operasi bisnis secepat mungkin setelah terjadi gangguan, termasuk pencadangan data yang teratur dan pengujian pemulihan bencana.

Peningkatan keamanan pada jaringan dan aplikasi

- **Keamanan jaringan**: Untuk menjaga keamanan jaringan dari serangan siber, organisasi dapat menggunakan sistem deteksi/pencegahan (EDR/XDR) untuk mendeteksi dan mencegah serangan. Selain daripada itu, segmentasi jaringan dan pembaruan perangkat secara berkala dapat membatasi dampak ancaman dan menutup celah keamanan.
- **Keamanan aplikasi**: memastikan bahwa perangkat lunak yang dikembangkan telah mempertimbangkan aspek keamanan, menguji aplikasi secara berkala untuk menemukan kelemahan, dan selalu memperbarui perangkat lunak dengan patch keamanan terbaru. Enkripsi data dan penggunaan Virtual Private Network (VPN) penting untuk melindungi informasi sensitif yang dikirim melalui jaringan.

Penilaian risiko siber

Penilaian risiko berkala membantu organisasi mengidentifikasi dan memprioritaskan ancaman serta kerentanan dalam sistem. Proses tersebut melibatkan penentuan ruang lingkup, identifikasi aset dan ancaman, serta evaluasi kontrol keamanan yang ada. Hasil penilaian dapat digunakan untuk mengembangkan strategi mitigasi risiko yang efektif untuk secara proaktif mengelola keamanan siber.

Manajemen identitas & akses

Manajemen identitas dan akses pengguna merupakan kunci keamanan siber yang memastikan bahwa akses kedalam sistem atau informasi hanya diberikan kepada individu yang membutuhkan. Penggunaan teknologi seperti Identity Access Management (PAM) hingga Multi Factor Authentication (MFA) dapat secara signifikan membantu Perusahaan mengelola akses pengguna dan meningkatkan keamanan siber.

Kontak PwC Indonesia

Subianto
Broader Assurance Services Leader
Chief Digital & Technology Officer
subianto.subianto@pwc.com

Andrew Tirtadjaja
Cybersecurity & Privacy Director
andrew.tirtadjaja@pwc.com

Daniel Septianto
Cybersecurity Senior Manager
daniel.s.septianto@pwc.com

Yudhi Ariyanto
Cybersecurity & Privacy Manager
yudhi.ariyanto@pwc.com

Ivan Kirsten
Cybersecurity & Privacy Manager
ivan.k.kirsten@pwc.com

Dimas Kusuma
Cybersecurity Manager
dimas.kusuma@pwc.com

BUMN Desk PwC Indonesia:

Yusron Fauzan
Partner
Assurance SOE Leader
yusron.fauzan@pwc.com

Firman Sababalat
Partner
Assurance Co-SOE Leader
firman.sababalat@pwc.com

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia

pwc