TINDAKAN PENCEGAHAN DAN RESPONS DASAR TERHADAP SERANGAN SIBER

FAIZAL HAQQI
MOCHAMAD SYAEFUL GHOZAL
ANDI ST FITRIANI

Pendahuluan

Dalam era digital yang semakin berkembang, ancaman siber menjadi semakin kompleks dan berbahaya, terutama bagi Aparatur Sipil Negara (ASN) yang bekerja dengan sistem informasi pemerintahan. Serangan siber dapat menyebabkan kebocoran data, gangguan operasional, hingga kerugian besar bagi organisasi dan masyarakat. Oleh karena itu, diperlukan pemahaman mendalam mengenai langkah-langkah pencegahan serta respons cepat dalam menghadapi insiden siber.

Buku modul ini dirancang untuk memberikan panduan praktis bagi ASN dalam menghadapi berbagai ancaman siber. Modul ini mencakup langkah-langkah pencegahan, prosedur jika akun atau sistem diretas, serta cara merespons insiden keamanan siber dalam pemerintahan. Dengan memahami materi ini, peserta pelatihan diharapkan dapat meningkatkan keamanan sistem informasi di lingkungan kerja masing-masing.

Penulis

Daftar Isi

BAB I
Langkah-langkah Pencegahan Serangan Siber untuk ASN

Pencegahan merupakan langkah utama dalam menghadapi ancaman siber. ASN sebagai bagian dari pemerintahan harus memahami cara melindungi sistem dan data dari berbagai serangan yang mungkin terjadi.

A. Prinsip Dasar Keamanan Siber untuk ASN

- **Gunakan Password yang Kuat**, kombinasikan huruf besar, huruf kecil, angka, dan simbol untuk meningkatkan keamanan.
- **Aktifkan Multi-Factor Authentication (MFA)**, tambahan lapisan keamanan untuk menghindari akses yang tidak sah.
- **Hindari Penggunaan Jaringan Wi-Fi Publik**, gunakan VPN jika harus mengakses sistem pemerintahan dari luar kantor.
- **Rutin Melakukan Update Perangkat dan Aplikasi**, Menutup celah keamanan yang dapat dimanfaatkan peretas.
- **Waspada terhadap Email Phishing dan Malware**, Jangan sembarangan membuka tautan atau lampiran mencurigakan.
- **Gunakan Perangkat Keamanan**, Pastikan firewall, antivirus, dan proteksi lainnya selalu aktif.
- **Edukasi dan Sosialisasi Keamanan Siber**, Lakukan pelatihan berkala agar ASN selalu waspada terhadap ancaman terbaru.

BAB II
Prosedur Dasar yang Harus Dilakukan Jika Akun atau Sistem Diretas

Meskipun telah melakukan langkah-langkah pencegahan, ada kemungkinan akun atau sistem tetap mengalami serangan siber. Oleh karena itu, penting bagi ASN untuk mengetahui prosedur dasar jika mengalami peretasan.

A. Langkah-langkah yang Harus Dilakukan Jika Akun Diretas

- **Segera Ubah Password**, Jika masih bisa mengakses akun, segera ganti password dengan yang lebih kuat.
- **Aktifkan MFA Jika Belum Digunakan**, MFA dapat mencegah akses ulang oleh peretas.
- **Laporkan ke Tim IT atau Pihak Berwenang**, Segera informasikan kejadian kepada tim keamanan siber.
- **Periksa Aktivitas Akun**, Cek log aktivitas untuk mengetahui kapan dan dari mana akses mencurigakan terjadi.
- **Keluar dari Semua Perangkat yang Terhubung**, Hindari akses lebih lanjut oleh pihak yang tidak bertanggung jawab.

B. Langkah-langkah yang Harus Dilakukan Jika Sistem Pemerintahan Diretas

- **Putuskan Koneksi Internet**, menghindari penyebaran serangan ke perangkat lain.
- **Identifikasi Sumber Serangan**, cek log keamanan untuk mengetahui bagaimana sistem disusupi.
- **Gunakan Backup Data**, jika data hilang atau terenkripsi, gunakan cadangan untuk memulihkan sistem.
- **Lakukan Forensik Digital**, investigasi lebih lanjut untuk memahami metode serangan dan memperbaiki celah keamanan.
- **Perbaiki dan Perbarui Sistem**, terapkan patch keamanan agar kejadian serupa tidak terulang.

BAB III
Insiden Keamanan Siber dalam Pemerintahan dan Cara Meresponsnya

Berikut adalah beberapa contoh insiden keamanan siber yang pernah terjadi di Indonesia:

- **Peretasan Situs DPR-RI (2017):**

Situs resmi Dewan Perwakilan Rakyat Republik Indonesia (DPR-RI) mengalami peretasan yang mengubah tampilan situs tersebut. Insiden ini menyoroti kerentanan dalam keamanan situs pemerintah. *Sumber : privy.id*

- **Kebocoran Data Pengguna Tokopedia (2020):**

Pada tahun 2020, data pengguna Tokopedia bocor dan diperjualbelikan di dark web. Kebocoran ini melibatkan jutaan data pengguna dan menekankan pentingnya perlindungan data pribadi. *Sumber : privy.id*

- **Serangan Ransomware pada Pusat Data Nasional (2024):**

Pada pertengahan tahun 2024, Pusat Data Nasional Sementara (PDNS) mengalami serangan ransomware yang mengakibatkan terganggunya layanan pemerintah dan menimbulkan sorotan tajam terkait keamanan data publik. *Sumber : techno.okezone.com*

- **Kebocoran Data Nomor Pokok Wajib Pajak (2024):**

Pada September 2024, terjadi dugaan kebocoran data Nomor Pokok Wajib Pajak (NPWP) yang melibatkan jutaan data, termasuk milik Presiden Joko Widodo dan para menterinya. Insiden ini menimbulkan kekhawatiran terkait potensi serangan siber yang lebih terarah. *Sumber : Reuters*

- **Gangguan pada Sistem e-Visa di Bandara Bali (2024):**

Pada tahun 2024, sistem e-visa di Bandara Bali mengalami gangguan yang mengakibatkan data sensitif pelancong, termasuk warga Australia, terekspos kepada pihak yang tidak berwenang. Insiden ini menyoroti perlunya peningkatan keamanan pada sistem imigrasi digital. *Sumber : News.com.au*

Insiden-insiden di atas menekankan pentingnya langkah-langkah pencegahan dan respons yang efektif terhadap ancaman siber, terutama bagi Aparatur Sipil Negara (ASN) yang terlibat dalam pengelolaan data dan sistem informasi pemerintahan.

Cara Merespons Insiden Keamanan Siber

Untuk mengatasi berbagai insiden keamanan siber di pemerintahan, berikut langkah-langkah umum yang dapat dilakukan:

- **Segera Isolasi Sistem yang Terinfeksi**, memutus akses ke jaringan untuk mencegah penyebaran serangan.
- **Lakukan Investigasi Cepat**, mengidentifikasi sumber dan metode serangan.
- **Laporkan ke Pihak Berwenang**, melibatkan tim keamanan IT dan lembaga terkait seperti BSSN.
- **Pulihkan Sistem dengan Backup Data**, jika memungkinkan, gunakan backup untuk memulihkan sistem yang terdampak.
- **Tingkatkan Keamanan Setelah Insiden**, menerapkan patch keamanan, mengubah kredensial, dan meningkatkan pemantauan sistem.
- **Edukasi Pegawai Tentang Insiden yang Terjadi**, agar serangan serupa dapat dicegah di masa mendatang.
- **Menyusun Rencana Kontingensi**, untuk memastikan kesiapan menghadapi insiden serupa di masa depan.

DAFTAR REFERENSI

- National Institute of Standards and Technology (NIST) - Panduan Keamanan Siber.
- Badan Siber dan Sandi Negara (BSSN) - Regulasi Keamanan Informasi di Indonesia.
- Buku “Cybersecurity Essentials” oleh Charles J. Brooks.
- Artikel dan jurnal terbaru mengenai ancaman siber dan strategi mitigasi.