Keamanan Siber dan Integritas Pilkada Serentak 2020

“Keamanan siber berkaitan dengan melindungi sistem, jaringan, perangkat lunak dan data yang terhubung ke internet, dari akses atau eksploitasi yang tidak sah. Keamanan siber juga berkaitan dengan teknologi pemilihan offline, serta melindungi integritas proses pemilihan dari informasi yang salah, yang mempengaruhi proses hasil oleh sistem.”

-Sam van der Stak & Peter Wolf

(*Cybersecurity in Elections Models of Interagency Collaboration*. 2019. Internasional IDEA).

7 Jenis Serangan Siber yang Kerap Terjadi selama Pemilu

1. Denial-of-Service (DoS) dan Distributed Dos (DDoS).
2. Mengubah tampilan website yang menayangkan hasil pemilihan.
3. Malware, ransomware, dan phishing.
4. Perusakan link komunikasi yang digunakan untuk mentransfer hasil penghitungan suara.
5. Perusakan integritas data pada Daftar Pemilih online.
6. Pembocoran data pribadi pemilih.
7. Kampanye disinformasi yang menargetkan integritas yang dirasakan dari proses pemilihan.

Antara Serangan Siber dan Kesiapan Sistem Teknologi

Risiko keamanan siber akan selalu ada, sehebat apapun sistem teknologi yang dibangun. Namun, sistem yang dipersiapkan menentukan bagaimana dampak serangan tersebut terhadap kerahasiaan, integritas, dan ketersediaan data dan teknologi.

Tren Pengamanan Siber di Berbagai Negara

Kolaborasi antarlembaga.

- ✓ Penyelenggara pemilu, pakar teknologi dan keamanan siber.
- ✓ Penyelenggara pemilu dan institusi pemerintah terkait.
- ✓ Penyelenggara pemilu, institusi pemerintah terkait, dan pihak swasta.
- ✓ Penyelenggara pemilu, institusi pemerintah terkait, pihak swasta dan platform media + media sosial.
- ✓ Penyelenggara pemilu, institusi pemerintah terkait, pihak swasta, platform media + media sosial, dan partai politik +kandidat.
- ✓ Penyelenggara pemilu, institusi pemerintah terkait, dan universitas + pakar teknologi dan keamanan siber.
- ✓ Penyelenggara pemilu, institusi pemerintah terkait, pihak swasta, platform media + media sosial, partai politik +kandidat, dan akademisi.

Yang penting diperhatikan

1. Kecukupan tenaga IT yang terlibat dalam e-rekap.
2. Pengaturan kontrol terhadap petugas atau pegawai yang bekerja pada lembaga penyelenggara pemilu.
3. Kategorisasi data.
4. *Back up* data secara berkala.
5. Memenuhi sertifikasi keamanan siber ISO 27001.
6. Sosialisasi dan edukasi keamanan siber.

Referensi

https://www.idea.int/sites/default/files/publications/cybersecurity-in-elections-models-of-interagency-collaboration.pdf

https://www.ria.ee/sites/default/files/content-editors/kuberturve/cyber_security_of_election_technology.pdf

https://www.sos.state.tx.us/elections/forms/election-security-best-practices.pdf