PERINGATAN KEAMANAN TERKAIT INDIKASI PENINGKATAN AKSI PERETASAN TERHADAP SISTEM ELEKTRONIK DI INDONESIA

RINGKASAN EKSEKUTIF

1. Tim Direktorat Operasi Keamanan Siber mendeteksi indikasi aksi serangan siber balasan yang dilakukan oleh kelompok peretas yang diindikasikan berasal dari Brazil. Hal ini berkaitan dengan upaya serangan balasan atas aksi peretas Indonesia terhadap sistem elektronik Brazil.
2. Berdasarkan hasil montoring sosial media, kelompok tersebut menargetkan sistem elektronik Kementerian dan Lembaga, Militer, Akademik, serta sektor lain di Indonesia.
3. Mengingat indikasi aksi serangan ini dan guna mengantisipasi dampak yang dtimbulkan, maka di imbau kepada seluruh pemangku kepentingan untuk meningkatkan kewaspadaan dan keamanan sistem elektronik yang dikelola dengan menerapkan langkah-langkah antisipasi yang diberikan pada Peringatan Keamanan ini.

LANGKAH-LANGKAH ANTISIPASI TERHADAP INDIKASI PENINGKATAN AKSI PERETASAN

Berkaitan dengan peningkatan tensi aksi peretasan terhadap sistem elektronik di Indonesia, Direktorat Operasi Keamanan Siber menghimbau seluruh penyelenggaran sistem elektronik untuk melakukan langkah-langkah sebagai berikut:

1. Menonaktifkan *port/services/plugin* pada sistem elektronik yang tidak digunakan untuk mencegah eksploitasi kerentanan dari *port/services/plugin* tersebut oleh pihak yang tidak bertanggung jawab.
2. Mengimplementasikan perimeter keamanan, seperti *Web Application Firewall* (WAF), *Intrusion Prevention System* (IPS)/*Intrusion Detection System*, Anti Virus/Malware serta melakukan pemantauan jaringan secara proaktif untuk setiap aktivitas yang mencurigakan, seperti percobaan serangan terhadap sistem elektronik yang dikelola.
3. Melakukan pencadangan terhadap data dan sistem elektronik yang dimiliki ke sistem penyimpanan yang terpisah/*offline* secara berkala.
4. Melakukan identifikasi kerentanan dan melakukan penerapan *patch security* secara berkala terhadap sistem elektronik yang dikelola khususnya untuk perimeter keamanan, jaringan, aplikasi, *database* maupun sistem operasi yang digunakan oleh komputer atau server yang menjadi sistem layanan yang dapat diakses oleh publik.
5. Melakukan penggantian password akun administrator maupun pengguna pada seluruh sistem elekteonik baik aplikasi, *database*, server dan lainnya secara

berkala dengan menggunakan password yang kuat serta menerapkan *multifactor authentication*.

6. Melakukan pengujian keamanan secara berkala terhadap seluruh sistem elektronik untuk mengidentifikasi kerentanan atau celah keamanan dan melakukan remediasi atau perbaikan terhadap celah keamanan yang dtemukan.
7. Melakukan langkah mitigasi awal dan Melaporkan kepada BSSN melalui Pusat Kontak Siber BSSN melalui email bantuan70@bssn.go.id. atau melalui telegram https://t.me/bantuan70 apabila menemukan indikasi anomali ataupun insiden yang terjadi pada sistem elektronik yang dikelola.