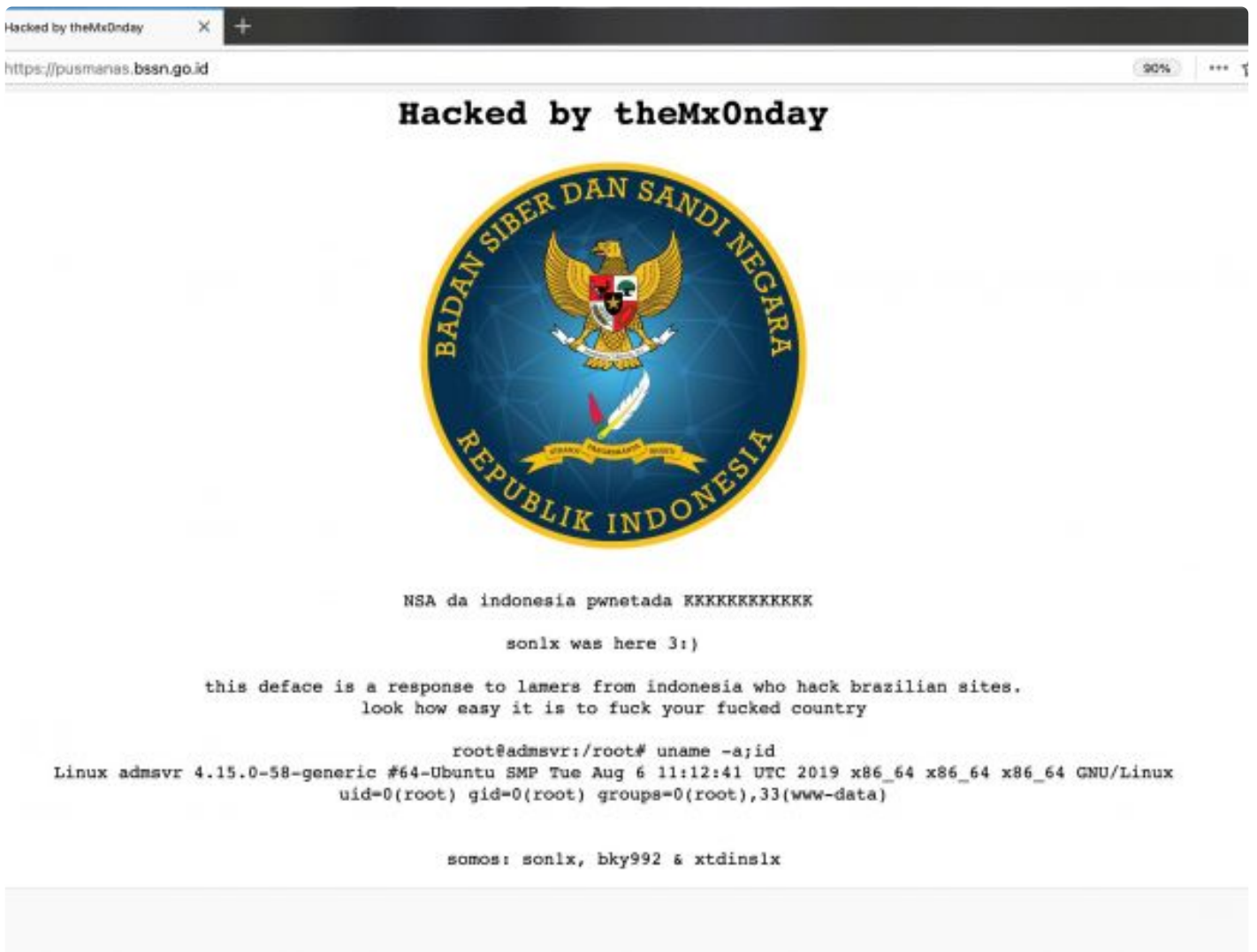


Giliran Situs Resmi BSSN Jadi Korban Peretasan

Pratama Persada - [INDONESIASATU.CO.ID](https://www.indonesiasatu.co.id)

Oct 25, 2021 - 15:16



JAKARTA - Serangan dengan deface memang sering terjadi ke website pemerintah, sebelumnya pada situs Setkab. Kali ini dikabarkan website BSSN (Badan Siber dan Sandi Negara) terkena deface, yang beralamat di www.pusmanas.bssn.go.id yang diketahui dari salah satu unggahan twitter.

Dalam keterangannya pada Senin (25/10), pakar keamanan siber Pratama Persada menjelaskan bahwa serangan tersebut diunggah pada hari rabu 20 oktober oleh akun twitter @son1x777. Di unggahan tersebut dituliskan telah di

hack oleh "theMx0nday".

"Ditulis oleh pelaku deface bahwa aksi ini dilakukan untuk membalas pelaku yang diduga dari Indonesia yang telah meretas website negara Brazil," terang chairman lembaga riset siber CISSReC (Communication & Information System Security Research Center) ini.

Pratama menambahkan bahwa, deface pada website merupakan peretasan ke sebuah website dan mengubah tampilannya. Perubahan tersebut bisa meliputi seluruh halaman atau di bagian tertentu saja. Contohnya, font website diganti, muncul iklan mengganggu, hingga perubahan konten halaman secara keseluruhan.

"Seharusnya BSSN sejak awal mempunyai rencana mitigasi atau BCP (Business Continuity Planning) ketika terjadi serangan siber, karena induk CSIRT (Computer Security Incident Response Team) yang ada di Indonesia adalah BSSN," terangnya.

Ditambahkan olehnya, kalau melihat sistem keamanan yang sudah baik di BSSN, sepertinya ada pelanggaran SOP terhadap link pada www.pusmanas.bssn.go.id, karena mungkin tidak melewati proses Penetration Test terlebih dahulu ketika akan di publish.

"Kalau di cek attack nya, mungkin bisa dicari tahu kenapa bisa firewallnya membypass serangan ke celah vulnerable nya. Attack yg simple pun, kalau lolos dari firewall bisa mengakibatkan kerusakan yang besar. Jangan dianggap semua serangan deface itu adalah serangan ringan, bisa jadi hackernya sudah masuk sampai ke dalam," kata pria asal Cepu, Kabupaten Blora, Jawa Tengah ini.

Menurut Pratama, perlu dilakukan digital forensik dan audit keamanan informasi secara keseluruhan. Sangat disayangkan BSSN sebagai institusi yang harusnya paling aman keamanannya, hanya gara-gara kesalahan kecil yang tidak perlu, ternyata jadi gampang diretas.

"Yang terpenting saat ini data di dalamnya tersimpan dalam bentuk encrypted. Jadi walaupun tercuri, hacker tidak akan bisa baca isinya," jelasnya

Ditambahkan olehnya, bahwa didalam dunia keamanan siber, tidak ada sistem informasi yang benar-benar aman 100%. Situs penting Amerika seperti FBI (Federal Bureau of Investigation) dan badan Antariksa Amerika, National Aeronautics and Space Administration (NASA) juga pernah diretas, lalu situs web badan intelijen Amerika, yaitu Central Intelligence Agency (CIA) pun juga menjadi korban serangan hacker.

"Salah satu solusinya yaitu, untuk security audit atau pentest bisa dilakukan secara berkala baik dengan pendekatan blackbox maupun white box. Metode yang digunakan bisa passive penetration atau active penetration," imbuhnya.

Dokter Pratama menambahkan, khusus untuk pentest Web Defacement, pengujian yang perlu dilakukan adalah Configuration Management Testing, Authentication Testing, Session Management Testing, Authorization Testing, Data Validation Testing dan Web Service Testing. Tools yg bisa digunakan

antara lain Arachni, OWASP Zed Attack Proxy Project, Websploit dan Acunetic.

Solusi lain secara kenegaraan adalah dengan menyelesaikan RUU PDP (Rancangan Undang Undang Perlindungan Data Pribadi) dengan segera. Jadi ada paksaan atau amanat dari UU PDP untuk memaksa semua lembaga negara melakukan perbaikan infrastruktur IT, SDM bahkan adopsi regulasi yang pro pengamanan siber. Tanpa UU PDP, maka kejadian peretasan seperti situs pemerintah akan berulang kembali. (***)