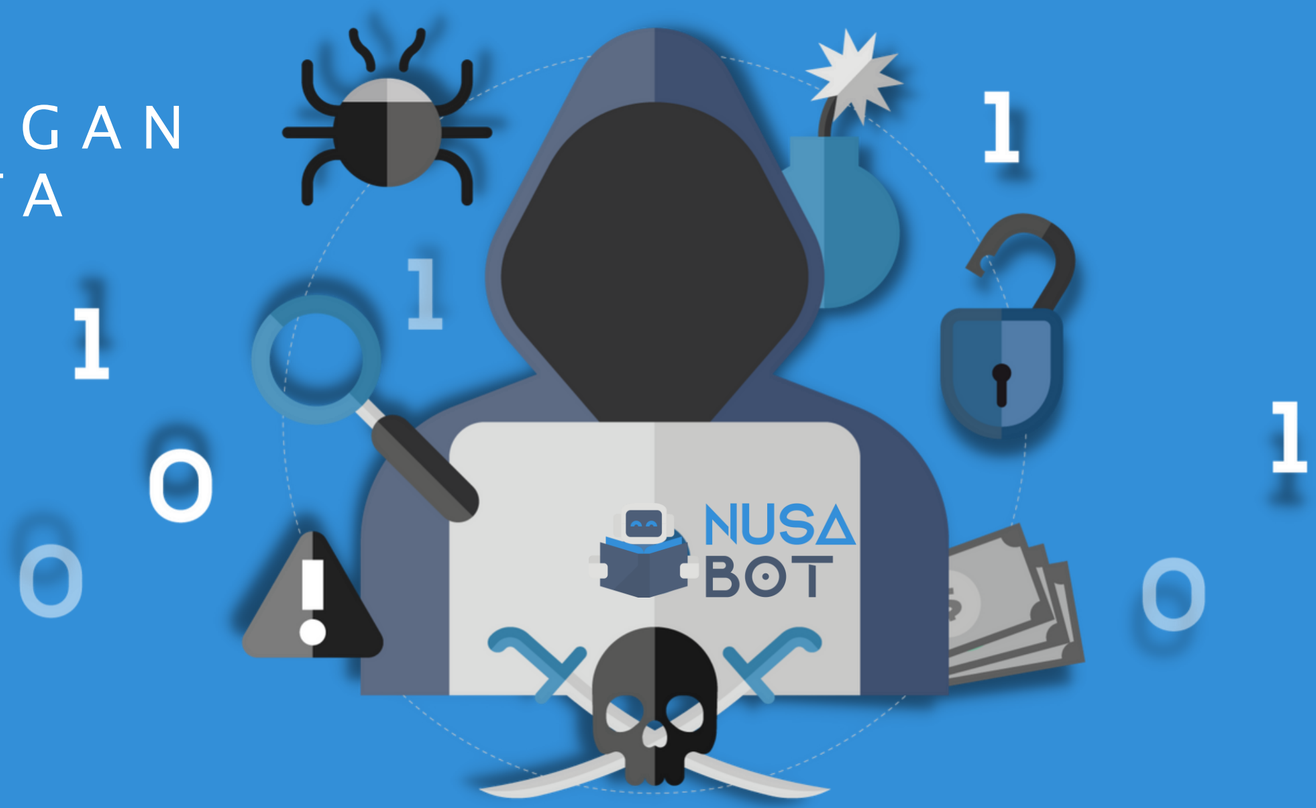
Mengamankan Perangkat IoT

CARA MENCEGAH SERANGAN DAN PELANGGARAN DATA



#JANGAN CUMA BISA COPY PASTE

Eugene Howard Spafford

The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards

Satu-satunya sistem yang benar-benar aman adalah yang dimatikan, dimasukan ke dalam beton dan disegel pada ruangan berlapis timah dengan penjaga yang bersenjata.

NUSA BOT

...You must consider every proprietary program as potential malware.

Anda harus mempertimbangkan bahwa setiap program *proprietary* (*closed-source*) memiliki potensi sebagai malware.

NUSA BOT

PENDAHULUAN

Alasan Keamanan IoT Penting

1. Kehilangan data pribadi.
2. Ancaman fisik.
3. Gangguan layanan.
4. Risiko kesehatan dan keselamatan.
5. Menjaga kepercayaan pengguna.
6. Ancaman keamanan nasional.

NUSA BOT

PENDAHULUAN

Tantangan Dalam Mengamankan Perangkat IoT

- Keterbatasan sumber daya.
- Ketergantungan pada protokol terbuka.
- Adanya kerentanan terhadap serangan dari dalam.
- Lambatnya pembaruan firmware.
- Tingkat kompleksitas tinggi.
- Minimnya kebijakan terhadap keamanan.

NUSA BOT

Ancaman Keamanan IoT

JENIS DAN STUDI KASUS

#JANGAN CUMA BISA COPY PASTE

Jenis Serangan Yang Mungkin Terjadi

- Man-in-the-Middle (MITM).
- Distributed Denial-of-Service (DDoS).
- Peretasan Sandi.
- Injeksi.
- Buffer Overflow.
- Serangan Melalui Jaringan Wi-Fi.
- Serangan Melalui Perangkat Lunak.

NUSA BOT

STUDI KASUS

SQL Injection

Strategi Keamanan IoT

- Memperbarui perangkat lunak dan firmware secara teratur.
- Memisahkan jaringan IoT dari jaringan utama.
- Membatasi akses ke perangkat IoT.
- Menonaktifkan fitur yang tidak diperlukan.

NUSA BOT

Implementasi keamanan IoT pada organisasi / perusahaan

LANGKAH YANG DIAMBIL SEBAGAI TINDAKAN PENCEGAHAN

#JANGAN CUMA BISA COPY PASTE

Implementasi keamanan IoT pada organisasi / perusahaan

- Menyusun kebijakan keamanan IoT.
- Melakukan pelatihan dan kesadaran tentang keamanan pada karyawan.
- Menerapkan sistem pemantauan dan deteksi ancaman keamanan IoT.

NUSA BOT

Menyusun Kebijakan Keamanan

- Identifikasi Risiko.
- Evaluasi Kebijakan Keamanan yang ada.
- Tentukan Tujuan dan Sasaran.
- Tentukan Langkah Keamanan.
- Evaluasi Kebijakan Keamanan secara Berkala.

NUSA BOT

Tindakan Lanjutan ?

YANG HARUS DILAKUKAN LAGI.

#JANGAN CUMA BISA COPY PASTE

Tindakan Lanjutan Yang Dapat Anda Lakukan

- Gunakan protokol keamanan yang sesuai.
- Perbarui perangkat IoT secara teratur.
- Gunakan enkripsi data.
- Monitoring keamanan secara terus-menerus.
- Buat kebijakan penggunaan perangkat IoT.
- Terus lakukan pelatihan dan kesadaran keamanan.

NUSA BOT