Keamanan Informasi dan Interoperabilitas Sistem Informasi RS dalam Era Endemi Covid-19 dan Revolusi Industri 4.0

Obrina Candra Briliyant, MT, CISA, CDPSE, CySA+, CSXF, ISO27001-LA, CyberOps

Politeknik Siber dan Sandi Negara, BSSN

"DOKUMEN ADALAH TIDAK BOLEH DISEBARLUASKAN DIUNDUH SECARA ONLINE"

Hospital Engineering Forum 2021

Indonesian Association Hospital Engineering

Curriculum Vitae

Nama: Obrina Candra Briliyant

Pendidikan:

- Akademi Sandi Negara
- Teknik Informatika ITB

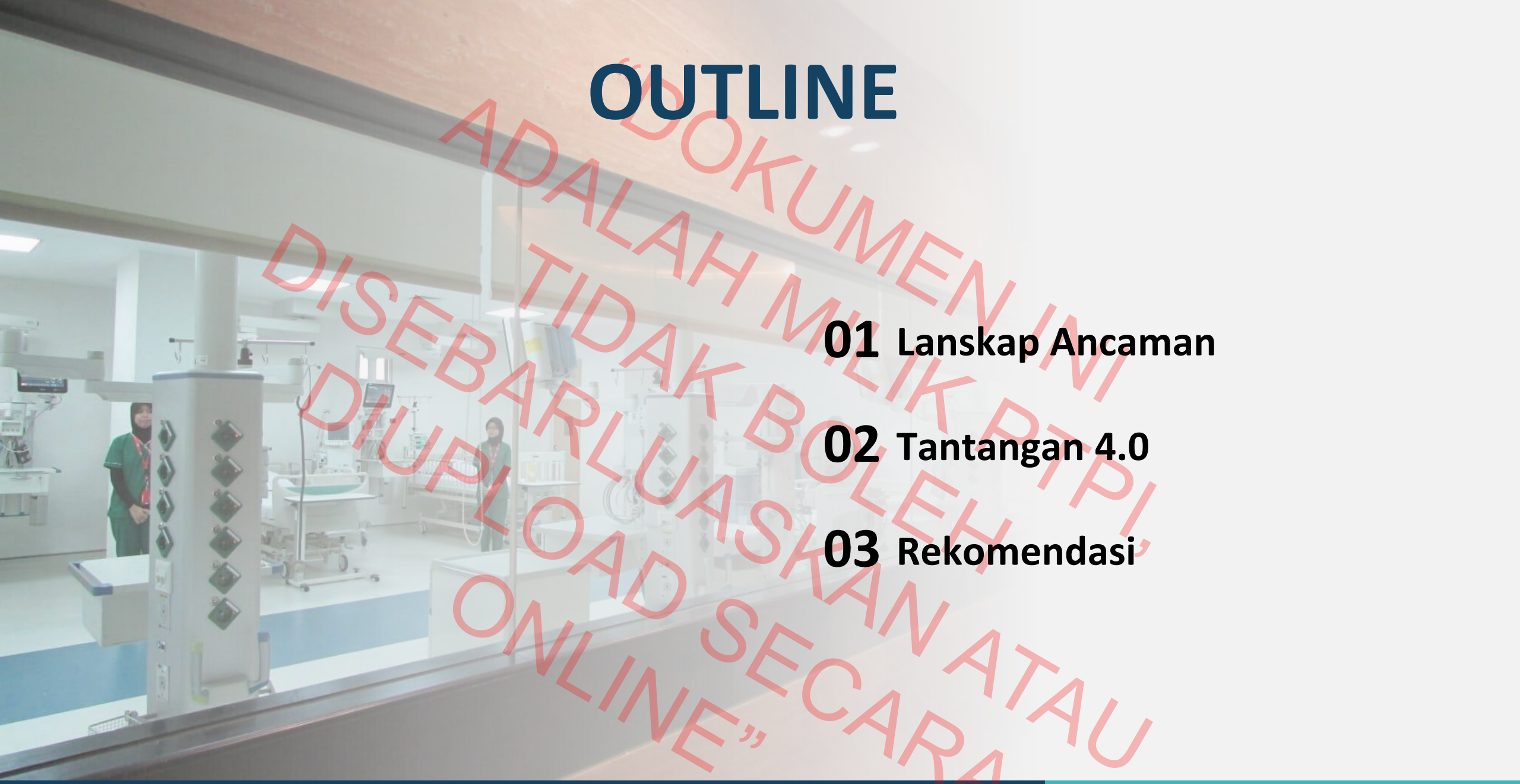
Pengalaman bekerja :

- Lembaga Sandi Negara
- Kemenko Polhukam RI
- Badan Siber dan Sandi Negara

Pengalaman organisasi :

- ISACA Indonesia Chapter
- Ikatan Auditor Sistem Informasi Indonesia

DOKUMEN INI ADALAH MILIK PTPI. TIDAK BOLEH DIGANDAKAN ATAU DIPUBLIKASIKAN SECARA "ONLINE"



OUTLINE

01 Lanskap Ancaman

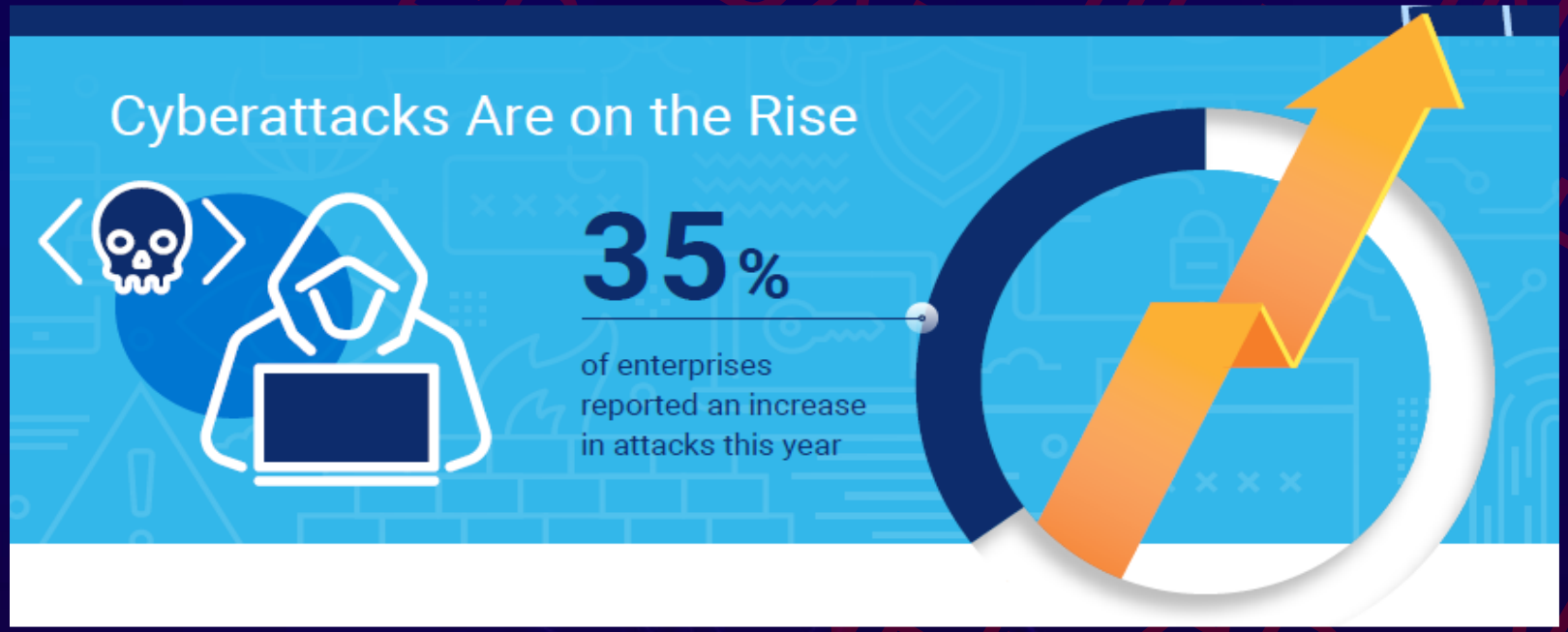
02 Tantangan 4.0

03 Rekomendasi

"DOKUMEN INI ADALAH MILIK RTPI, TIDAK BOLEH DISEBARLUASKAN ATAU DIUPLOAD SECARA ONLINE"

1 Lanskap Ancaman

ISACA *State of Cybersecurity* 2021 melihat pada tren ancaman, dampak pandemi pada program keamanan, serta pentingnya menilai kematangan *cybersecurity*. Banyak dari temuan ini akan memperkuat tantangan lama & baru yang dihadapi organisasi di tengah pandemi global yang sedang berlangsung dan aktor ancaman oportunistik.



- 1 dari 3 organisasi mengalami lebih banyak serangan siber tahun ini
- tiga poin lebih tinggi dari tahun lalu

www.isaca.org/state-of-cybersecurity-2021

- di mana ada konektivitas, ada risiko serangan siber
- Serangan langsung pada teknologi operasional (OT/ICS, SCADA) jarang terjadi karena sistem ini biasanya lebih terlindungi
- Kemungkinan besar peretas memperoleh akses ke sistem komputer melalui sisi administratif bisnis

Some of the biggest attacks we've seen all started with an email

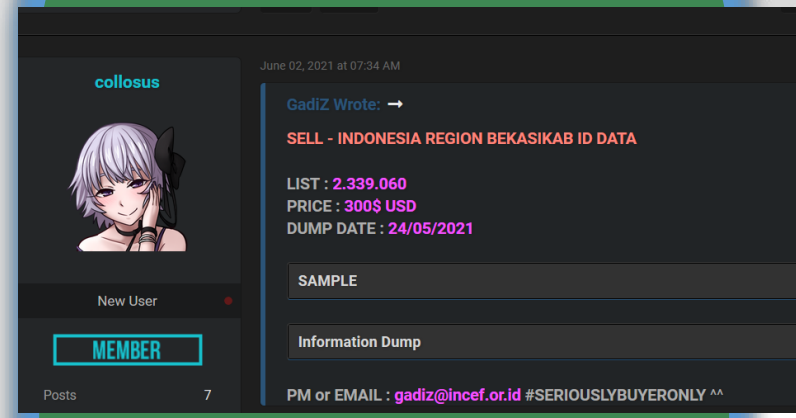
- Colonial Pipeline dilaporkan membayar US$4,4 juta sebagai tebusan kepada para aktor DarkSide.
- Perusahaan memiliki asuransi cyber dengan Lloyd's dan Beazley, yang menanggungnya setidaknya US$15 juta.
- Pada 2019, Norsk Hydro menerima US$20,2 juta dalam asuransi siber dari AIG.
- Laporan keamanan tahun 2020 dari Cybereason menunjukkan bahwa 80% organisasi yang membayar uang tebusan, mengalami serangan kedua.

"DOKUMEN INI ADALAH MILIK PTPN III (PERSERO) DAN BERSIFAT RAHASIA. DILARANG MENYEBARLUASKAN ATAU MENGGUNAKAN SEBAGIAN ATAU SELURUH ISI DOKUMEN INI SECARA ONLINE"

INSIDEN SIBER DI INDONESIA

Isu kebocoran data warga Indonesia yang diduga merupakan data BPJS Kesehatan pertama kali mencuat di media sosial pada Kamis (20/5/2021). Data itu dipublikasikan dan dijual di salah satu forum online.

Juli 2021, Data nasabah asuransi BRI Life diduga bocor dan dijual di darkweb. Dalam unggahan sampel data, disertakan screenshot yang berisi data milik nasabah BRI Life, seperti KTP hingga rekam medis. Ditemukan bukti beberapa komputer milik karyawan BRI Life telah menjadi sarana hacker dalam melakukan pembobolan data ini.



Mei – Juni 2021, serangkaian laporan penjualan data hasil breach beberapa pemerintah daerah dan BUMD bermunculan di darkweb. Penjual mengklaim menjual data pribadi berupa nik, kk, dan nama ibu kandung.

Most Frequent Cyberattacks

experienced by respondents are:

1. **14%** Social engineering
2. **10%** Advanced persistent threat (APT)
3. **9%** Ransomware
3. **9%** Unpatched system
4. **8%** Denial of service (DoS)
4. **8%** Security misconfiguration

Top 5 of attacks are the same as last year

GLOBAL RANSOMWARE INCIDENTS

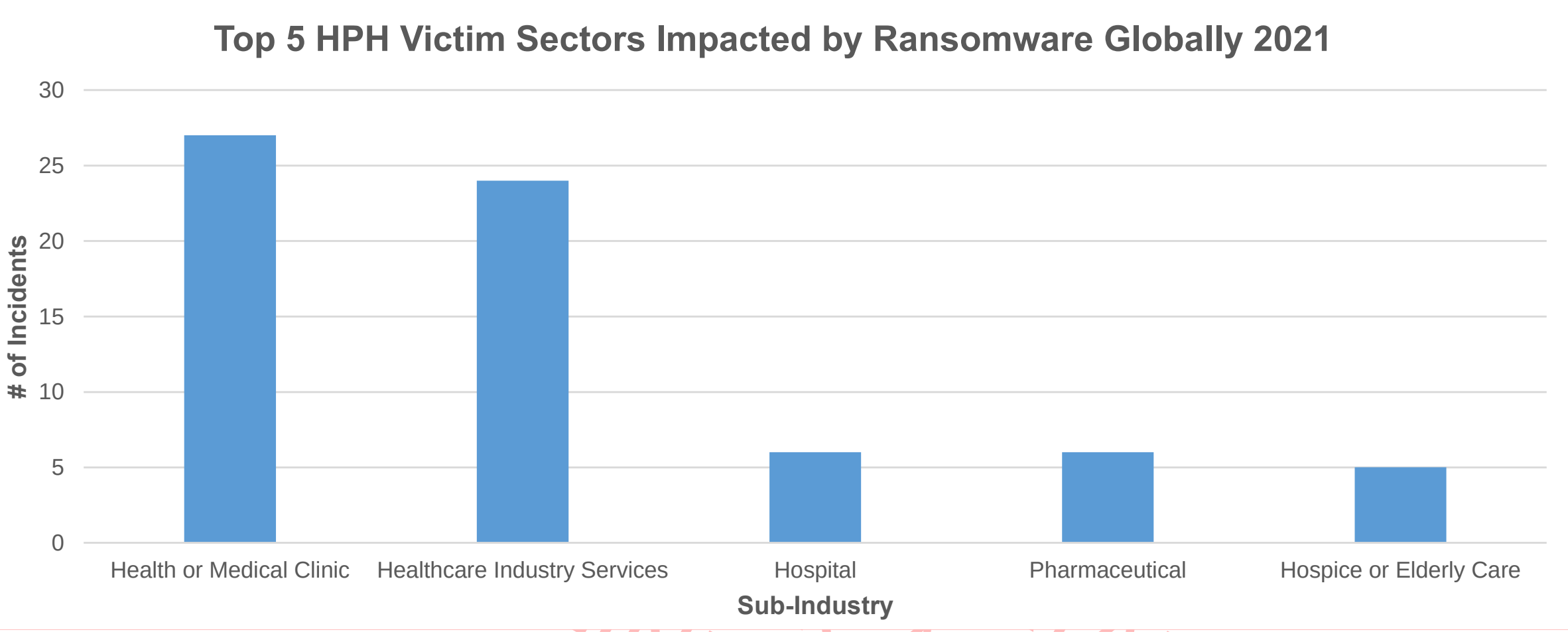
Top 5 Ransomware Actors Impacting Global HPH Sector 2021		
Place	**RaaS Name**	**Number of Incidents**
1	Avaddon RaaS Operator(s)	16
2	Conti RaaS Operator(s)	16
3	REvil/Sodinokibi RaaS Operator(s)	7
4	Mespinoza/Pysa RaaS Operator(s)	6
5	Babyk RaaS Operator(s)	5

RaaS -> Ransomware as a Service

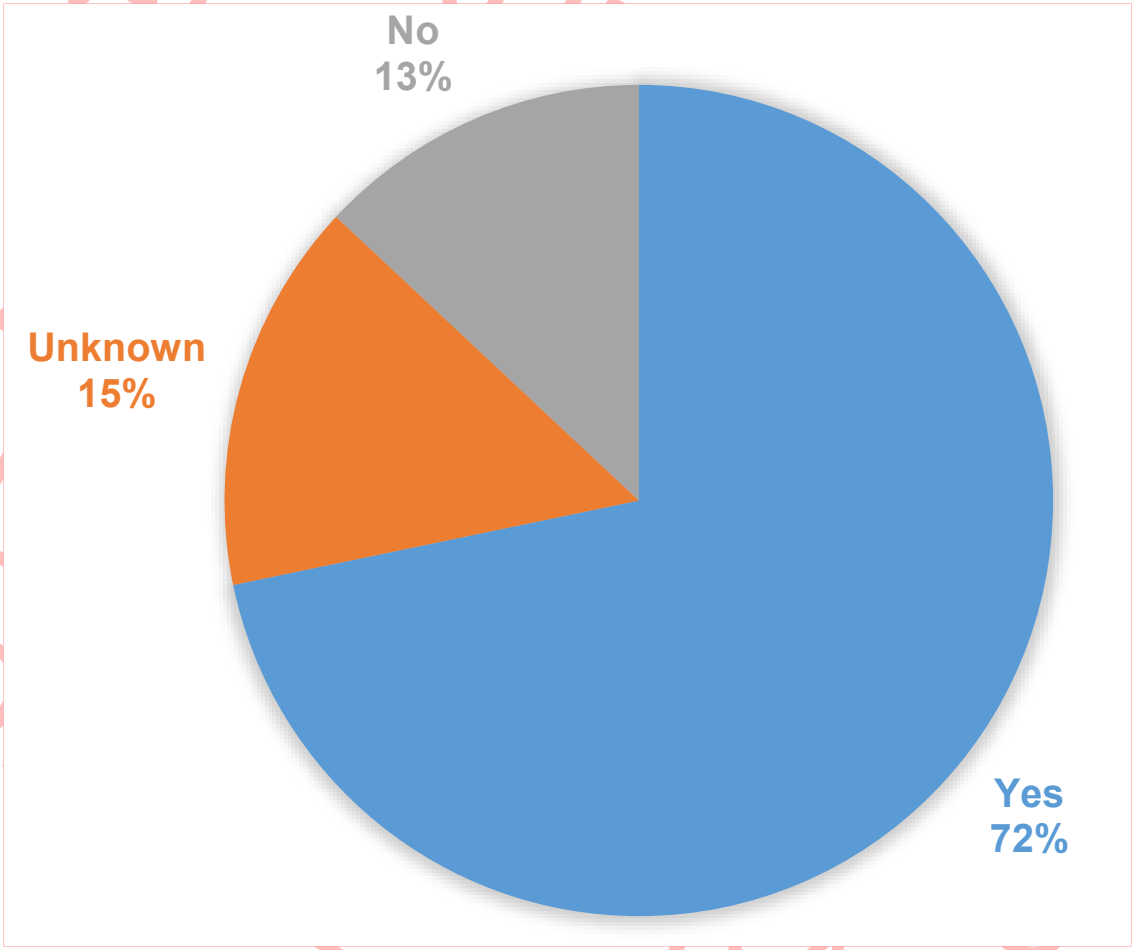
https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

- *Health Sector Cybersecurity Coordination Center* (HC3) dibuat oleh Departemen Kesehatan AS untuk membantu perlindungan informasi kesehatan (e-PHI) di seluruh Sektor Kesehatan dan Kesehatan Masyarakat/*Health and Public Health Sector* (HPH).
- Karena daya tarik sektor HPH bagi pelaku ransomware, tim HC3 memberikan perhatian khusus pada tren ransomware.
- HC3 telah melacak total **82** insiden ransomware yang berdampak pada sektor perawatan kesehatan di seluruh dunia sepanjang tahun 2021 ini, per 25 Mei 2021.
- Temuan didasarkan terutama pada pengamatan blog aktor ransomware, tetapi juga pelaporan media sumber terbuka dan *breach notification*.

"DOKUMEN INI ADALAH MILIK PTPI, DILARANG DISEBARLUASKAN SECARA ONLINE"


Top 5 HPH Victim Sectors Impacted by Ransomware Globally 2021
# of Incidents
30
25
20
15
10
5
0
Health or Medical Clinic
Healthcare Industry Services
Hospital
Pharmaceutical
Hospice or Elderly Care
Sub-Industry

INSIDEN RANSOMWARE HPH 2021: APAKAH DATA DIBOCORKAN PELAKU?



DISEBARKAN
DIUPL

Serangan terhadap Sistem Kesehatan Irlandia

- Departemen Kesehatan Irlandia dan Eksekutif Layanan Kesehatan (HSE) diserang oleh ransomware Conti pada Mei 2021
- Penasihat klinis nasional HSE Dr. Vida Hamilton mengatakan hal itu "mempengaruhi setiap aspek perawatan pasien"
- Gangguan paling berdampak terhadap layanan rawat inap dan layanan penerbitan akta kelahiran dan kematian
- Fasilitas kesehatan terpaksa kembali menggunakan dokumentasi kertas
- Data pasien dirilis secara online

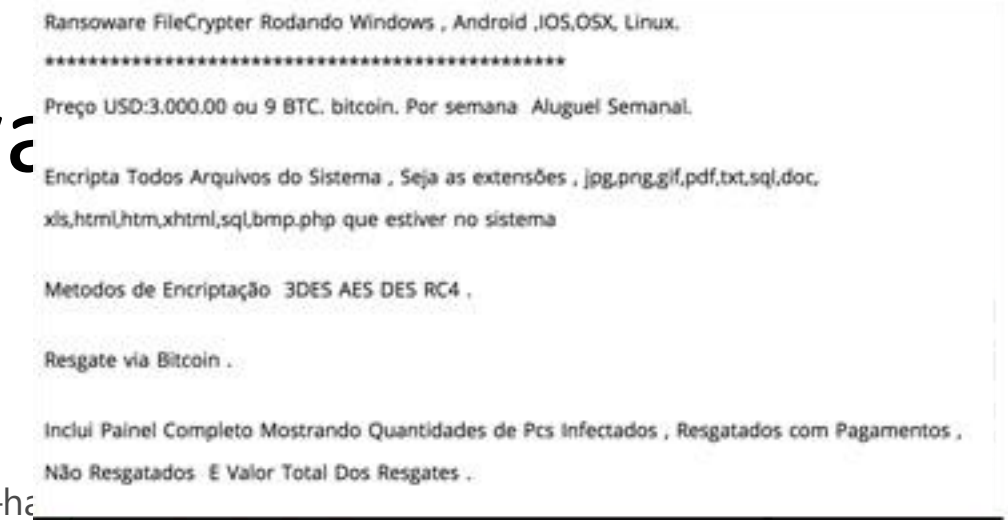
https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

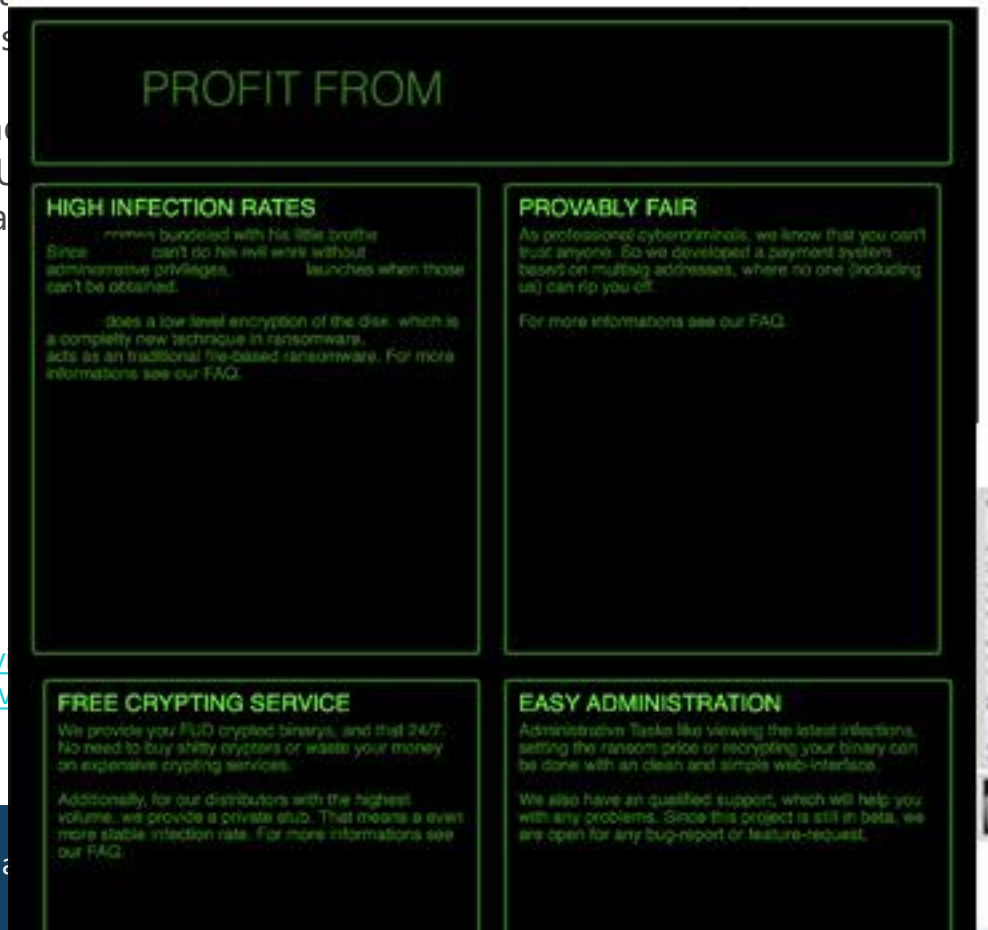
"DOKUMEN INI ADALAH MILIK PTRI DILARANG DIBOLEHKAN DISEBARKAN ATAU DIGUNAKAN SECARA ONLINE"

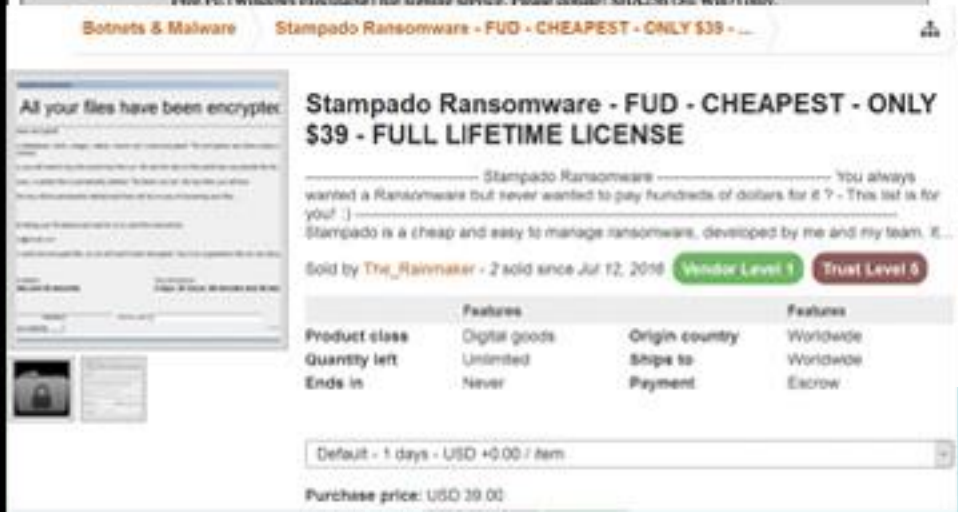
Malwa

CryptoWall—ha
jenis/*strain* rans
antara ratusan,
dengan $39 pa
menghasilkan U
dari para korba

https://www.trendmicro.com/v
threats/ransomware-as-a-serv

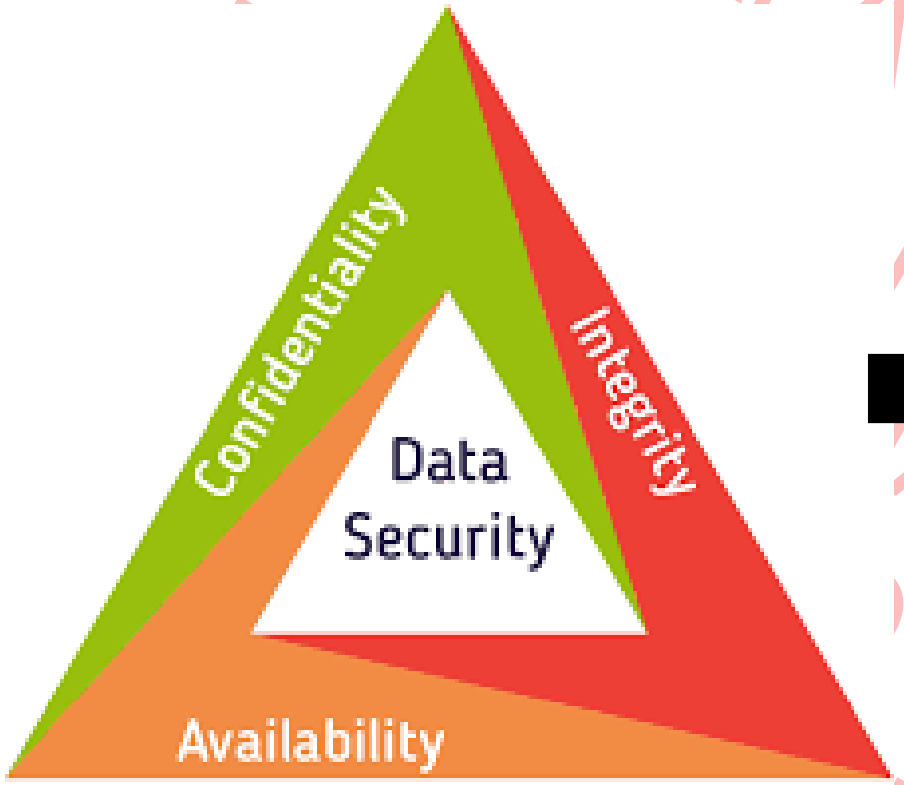






2 Tantangan 4.0

the devil is in the details



"DOKU ADAI NH M KR ASK SEC E"

Healthcare IT Challenges

Healthcare telah mengalami modernisasi TI yang signifikan. Berikut 4 tantangan Keamanan Data pada *Healthcare :*

1. **Integrasi jaringan**. Di sisi bisnis *healthcare*, ada banyak merger dan akuisisi, atau adopsi alkes berbasis elektronik/bahkan IP. Sayangnya, hal ini sering menyebabkan masalah integrasi jaringan dan visibilitas jaringan.
2. **Perawatan pasien jarak jauh**. Penelitian terbaru menunjukkan bahwa 71% dari semua penyedia *healthcare* menggunakan alat kesehatan jarak jauh atau pengobatan jarak jauh untuk terhubung dengan pasien.
3. **Kepatuhan terhadap Regulasi/Standar**. Indonesia belum memiliki regulasi khusus untuk PHI, namun data rekam kesehatan WNI dilindungi sesuai UU 24/2013 ttg Adminduk pasal 84. AS memiliki HIPAA (*Health Insurance Portability and Accountability Act of 1996*) yang sangat ketat dalam masalah seperti *breach* informasi pribadi pasien yang melanggar hukum, dan setiap insiden *data breach* yang dapat berakibat denda besar atau kerusakan reputasi yang signifikan.
4. **Perencanaan respon insiden siber**. Memiliki rencana untuk menangani ransomware sangat penting untuk organisasi *healthcare*. Meskipun enkripsi dan *backup* penting, itu mungkin tidak cukup. Organisasi yang *comply* terhadap standar seperti HIPAA atau ISO 27001 akan melihat manfaat terbesar.

Pasal 84

(1) Data Pribadi Penduduk yang harus dilindungi memuat:

a. keterangan . . .

PRESIDEN
REPUBLIK INDONESIA

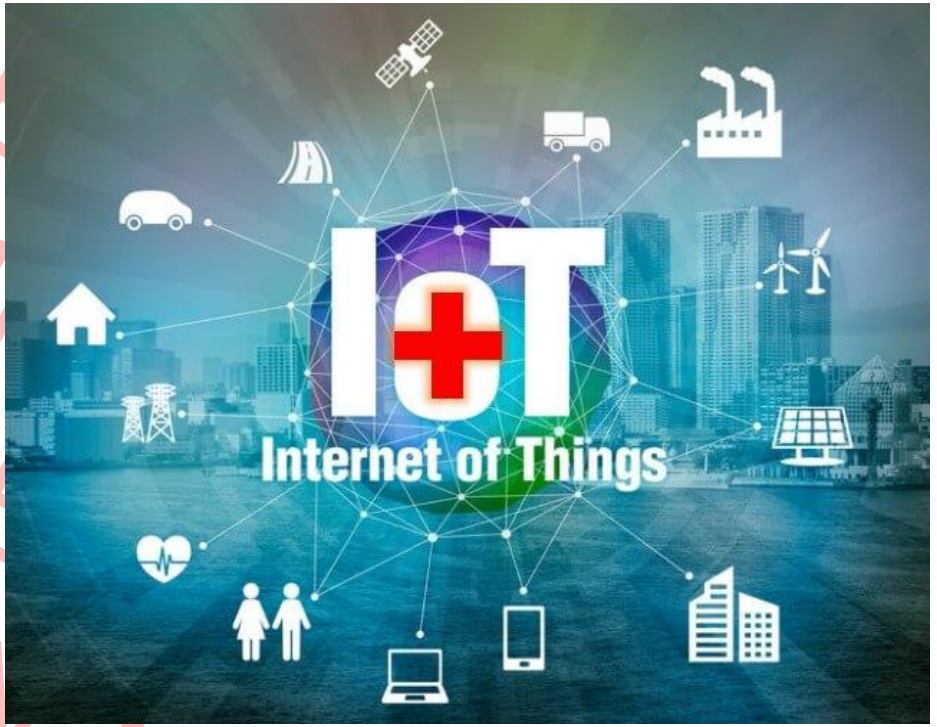
- 21 -

a. keterangan tentang cacat fisik dan/atau mental;
b. sidik jari;
c. iris mata;
d. tanda tangan; dan
e. elemen data lainnya yang merupakan aib seseorang.

"DOKUMEN INI ADALAH MILIK PRIBADI TIDAK BOLEH DISEBARLUASKAN ATAU DIUPLOAD SECARA ONLINE"

The Rise of IoTs

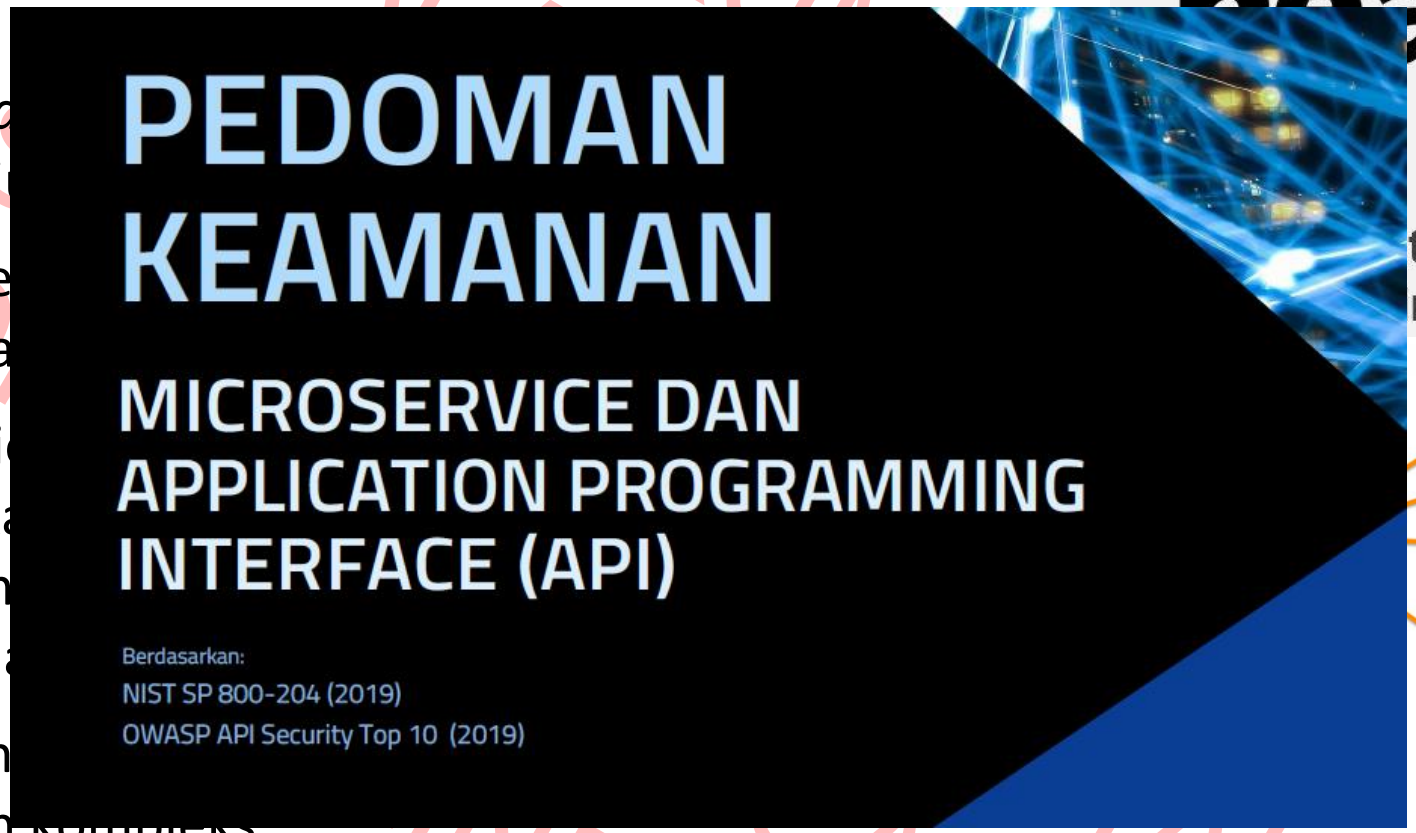
- Dalam banyak hal, sistem IoT sangat mirip dengan tubuh manusia – sistem besar dan kompleks yang selalu aktif.
- Mari kita gunakan serangan jantung sebagai analogi. Kita semua tahu bahwa serangan jantung bisa menjadi bencana besar. Meskipun serangan jantung biasanya terjadi secara tiba-tiba, kondisi yang memungkinkannya sebenarnya membutuhkan waktu berhari-hari, berbulan-bulan atau bahkan bertahun-tahun untuk terbentuk.
- Jika kita dapat secara terus menerus, otomatis dan cerdas memantau jantung dan tubuh, kita dapat mendeteksi tanda-tanda awal masalah dan mengambil tindakan pencegahan untuk menghindari serangan jantung.
- Sayangnya, banyak Unit TIK organisasi tidak memiliki informasi serupa di jaringan IoT. Sebagian besar rumah sakit tidak memiliki informasi terkini tentang jenis perangkat IoT apa yang mereka miliki, apalagi berapa banyak perangkat ini yang terhubung ke jaringan mereka. Jadi, visibilitas perangkat IoT adalah **tugas pertama** untuk setiap organisasi.



"DOKUMEN INI ADALAH MILIK BOLEH TIDAK BOLEH DISEBARLUASKAN ATAU DIUPLOAD SECARA ONLINE"

Securing the Connecting Doors

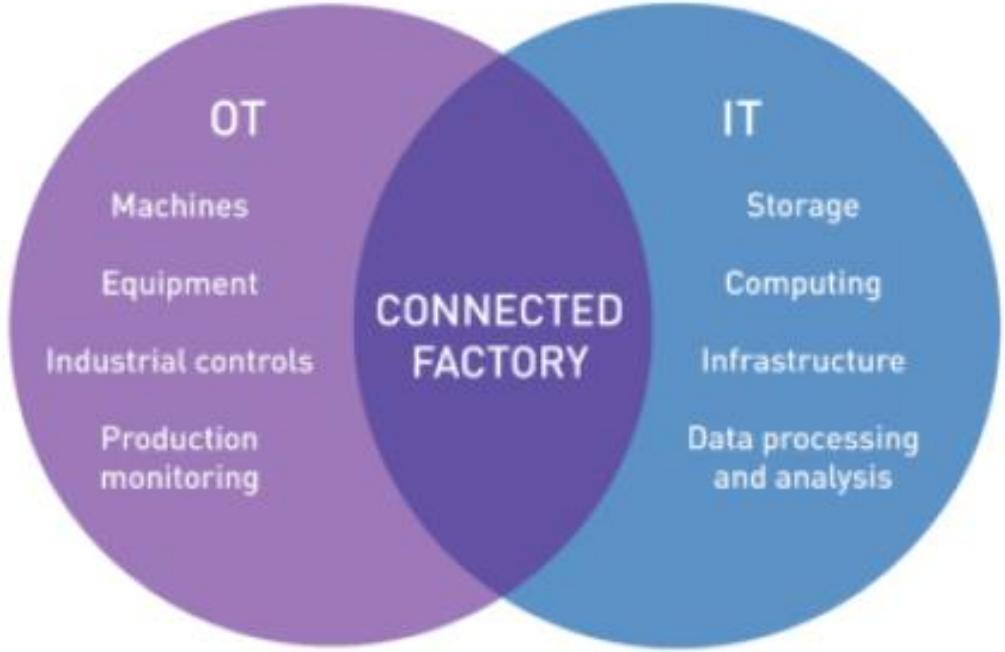
- *MyHealthEDa*
  walaupun tuj
- Masalah akse
  dari keamana
- API (applicati
  memungkinka
  ketiga, dan m
  tersedia di ma
- Tetapi ancam
  menjadi lebih kompleks.



"DOKU
ADALA
DI
INE" CARA

Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift

- Cloud dan Shadow IT memberi dampak attack vector baru
- Konvergensi OT –> IT, e.g. *Building Automation System* (BAS), Robotik, *Medical Devices Data System* (MDDS)
- Keamanan TI konvensional masih berbasis Perimeter



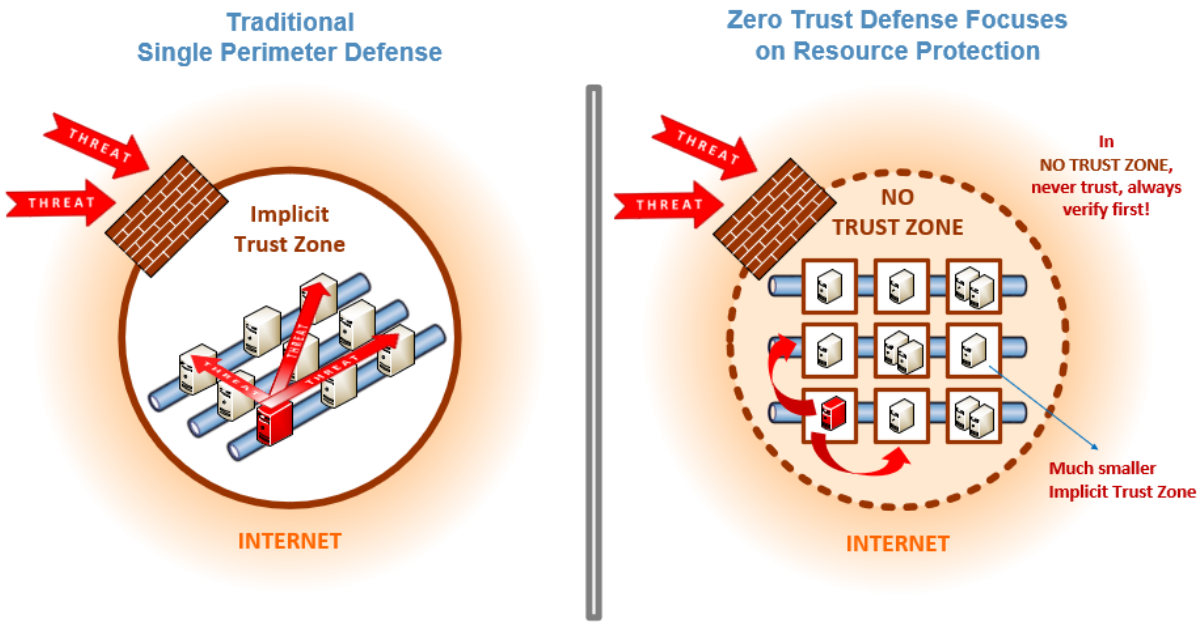
"DOKUMEN INI ADALAH MILIK ... TIDAK BOLEH DISEBARLUASKAN ATAU DIUPLOAD SECARA ONLINE"

https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/healthcare-securitythree-paradoxes-and-the-need-for-a-paradigm-shift

3 Rekomendasi

TAKEAWAYS

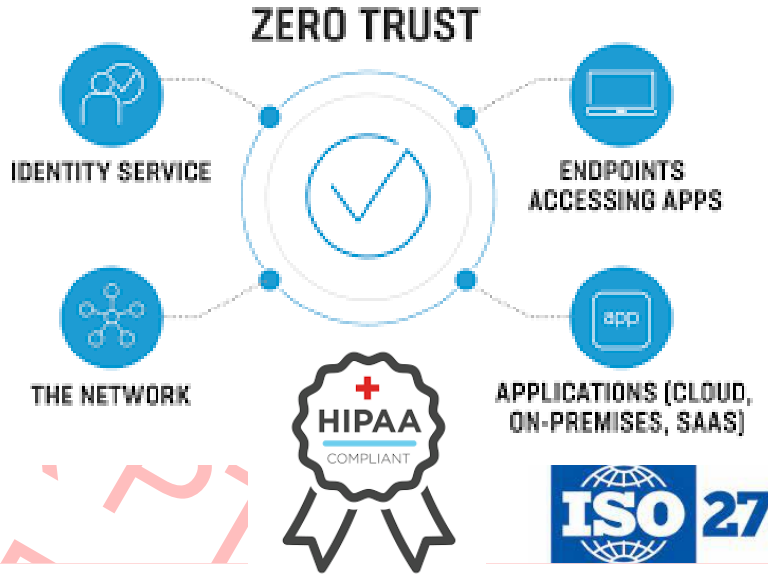
- Dalam ekosistem di mana sistem TI tradisional berdampingan dengan sistem *shadow IT* (BYOD, mobile apps, GDocs) dan sistem manajemen data lainnya (cloud, MDDS, SCADA), perlindungan data dan infrastruktur penting harus ditangani dari sudut pandang yang berbeda.
- Metafora yang tepat mungkin adalah kota terbuka dengan sejumlah bangunan kritis, bukan benteng berdinding. Tujuan keamanan tidak lagi pertahanan benteng, melainkan perlindungan bangunan kritis dalam suatu kota terbuka.
- Semua teknologi informasi dan otomatisasi di rumah sakit harus menjadi pertimbangan. Keamanan harus meliputi TI tradisional, cloud, alkes, otomatisasi bangunan, dan shadow IT lainnya.



ARSIP TIDAK BERLAKU
DISEBARLUASKAN ATAU
DIUPLOAD SECARA
ONLINE"

Rekomendasi

1. **Raise Awareness**. Manusia – yaitu pengguna akhir – akan selalu menjadi mata rantai terlemah.
2. **Govern your Security**. Organisasi/fungsi keamanan TI akan menjadi ujung tombak program keamanan anda.
3. **Apply Zero Trust.** Pergeseran keamanan konvensional berbasis perimeter ke arah keamanan berbasis hak akses merupakan kondisi ideal.
4. **Invest in Predictive Analysis.** Platform *Cyber Threat Intelligence* (CTI) dapat menyediakan analisis *real-time* tentang deteksi dan respon insiden. Kerjasama sektoral juga menjadi kunci kesuksesan keamanan.



"DOKUMEN INI ADALAH MILIK PT. [illegible] TIDAK BOLEH DISEBARLUASKAN DIUPLOAD SECARA ONLINE"

Thank You