16º SEMINÁRIO FEMIPA

FILANTRÓPICOS FORTALECIDOS, POPULAÇÃO BEM ASSISTIDA

19, 20 E 21 DE MARÇO 2024 - CURITIBA / PR

ATAQUE CIBERNÉTICO: QUAIS OS RISCOS REAIS PARA OS HOSPITAIS

Glaucio Erlei de Souza
Hospital Nossa Senhora das Graças

Sobre o hospital

70 anos
NOSSA SENHORA DAS GRAÇAS HOSPITAL

Quem somos

O **Hospital Nossa Senhoras das Graças**, é um hospital geral, filantrópico, referência em procedimentos de alta complexidade, como cirurgia robótica, transplante de medula óssea e hepático. É um completo centro Hospitalar, com apoio diagnóstico e de tratamento para as diversas especialidades.

Sobre o grupo hospitalar

GRUPO HOSPITALAR nossa senhora das graças

NOSSA SENHORA DAS GRAÇAS HOSPITAL

MATERNIDADE Mater Dei GRUPO HOSPITALAR NSG

HOSPITAL DA Providência Unidade Materno Infantil GRUPO HOSPITALAR NSG

HOSPITAL DA Providência GRUPO HOSPITALAR NSG

Hospital Infantil Dr. Jeser Amarante Faria

Quem somos

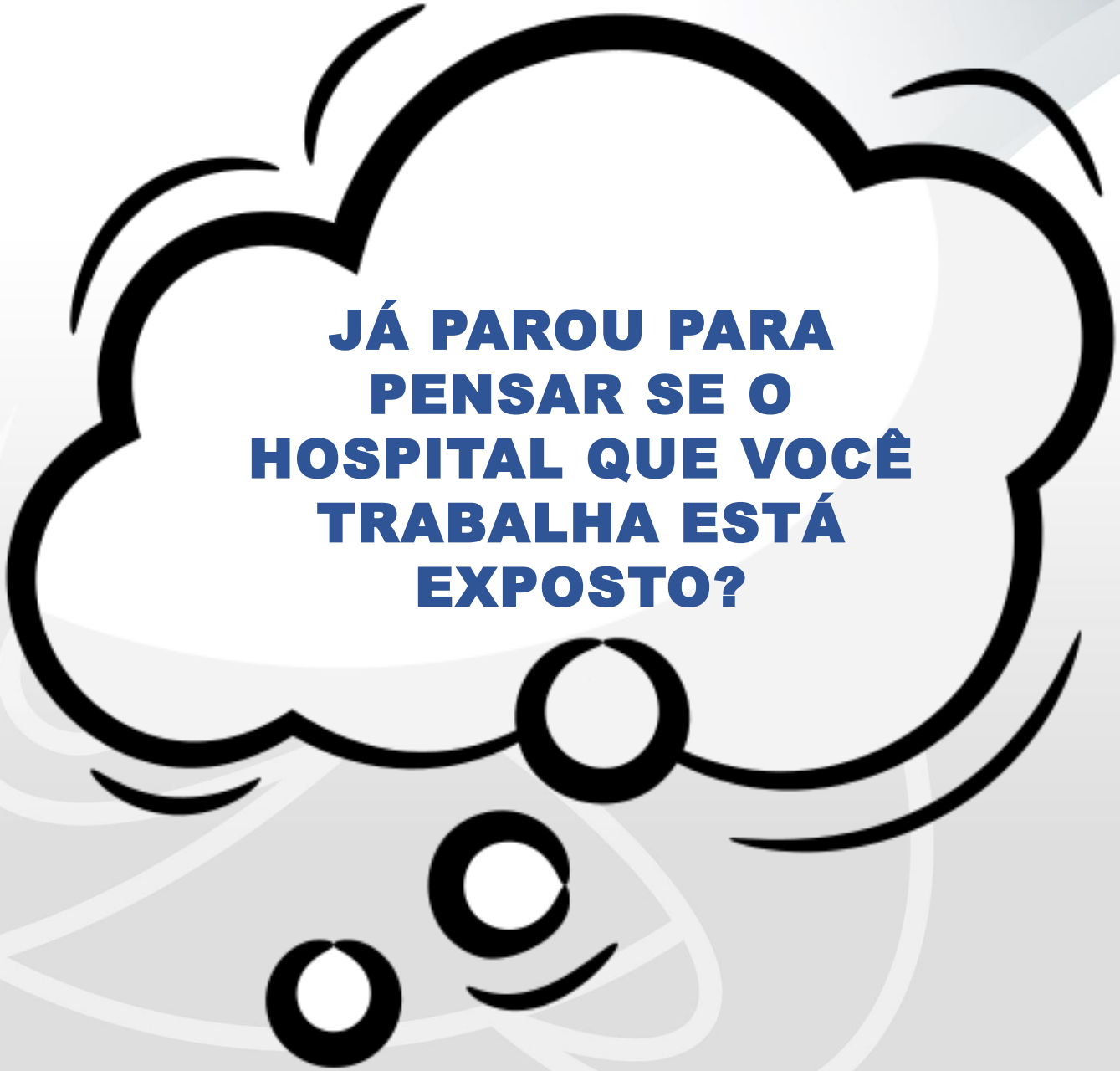
O HNSG faz parte do Grupo Hospitalar Nossa Senhora das Graças, sendo responsável pela gestão de outros 4 Hospitais, que atendem em sua maioria usuários do SUS.

850 leitos

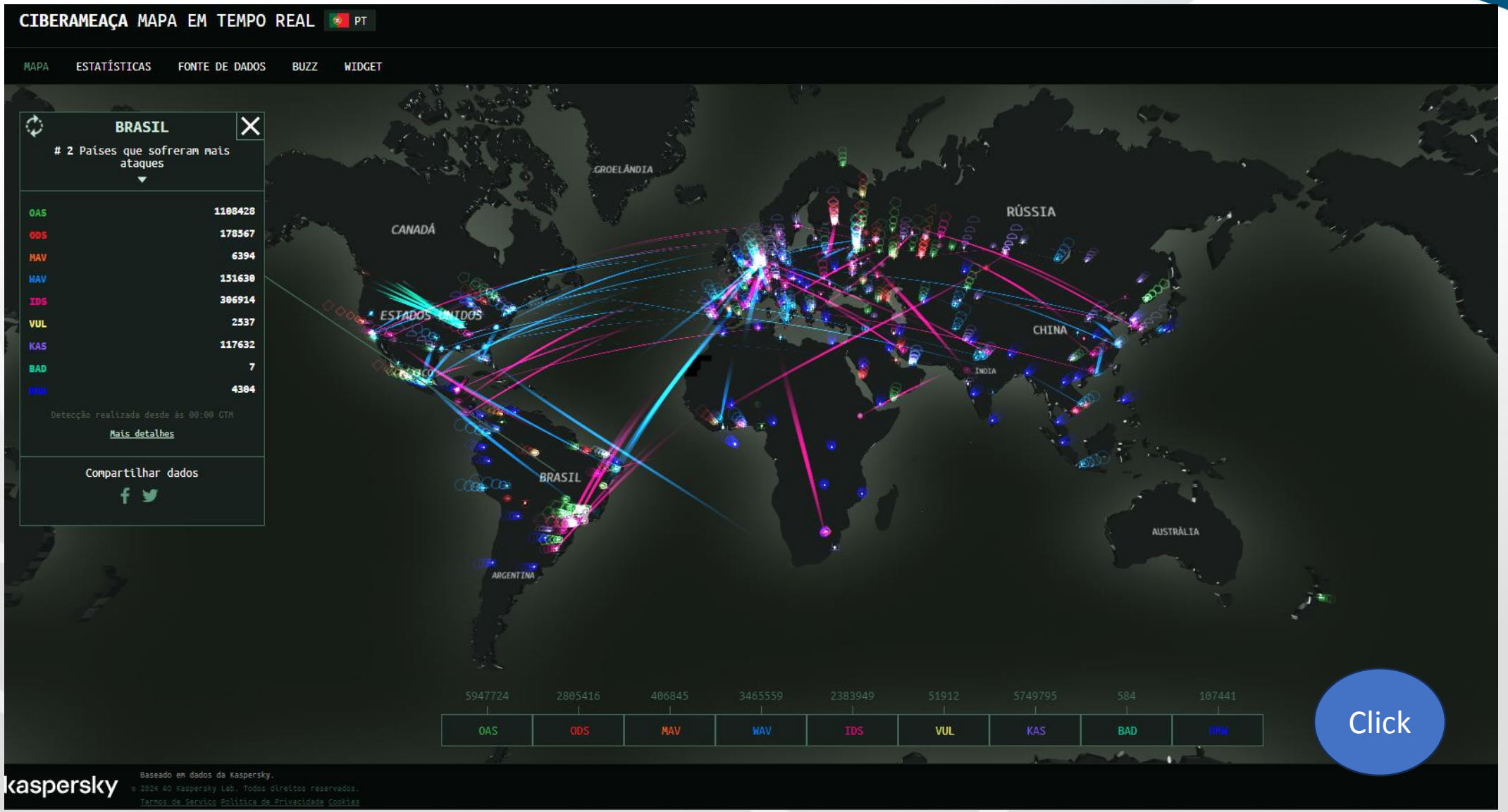
+60k INTERNAÇÕES

Fontes: HNSG (2023)

ATAQUE CIBERNÉTICO: QUAIS OS RISCOS REAIS AS EMPRESAS?


JÁ PAROU PARA PENSAR SE O HOSPITAL QUE VOCÊ TRABALHA ESTÁ EXPOSTO?

Retrospectiva



https://cybermap.kaspersky.com/pt

Contexto 2020 – Ataques cibernéticos com repercussão na mídia*

- Casos Divulgados

Contexto Atual – Incidentes de segurança com repercussão na mídia*

- Casos Divulgados

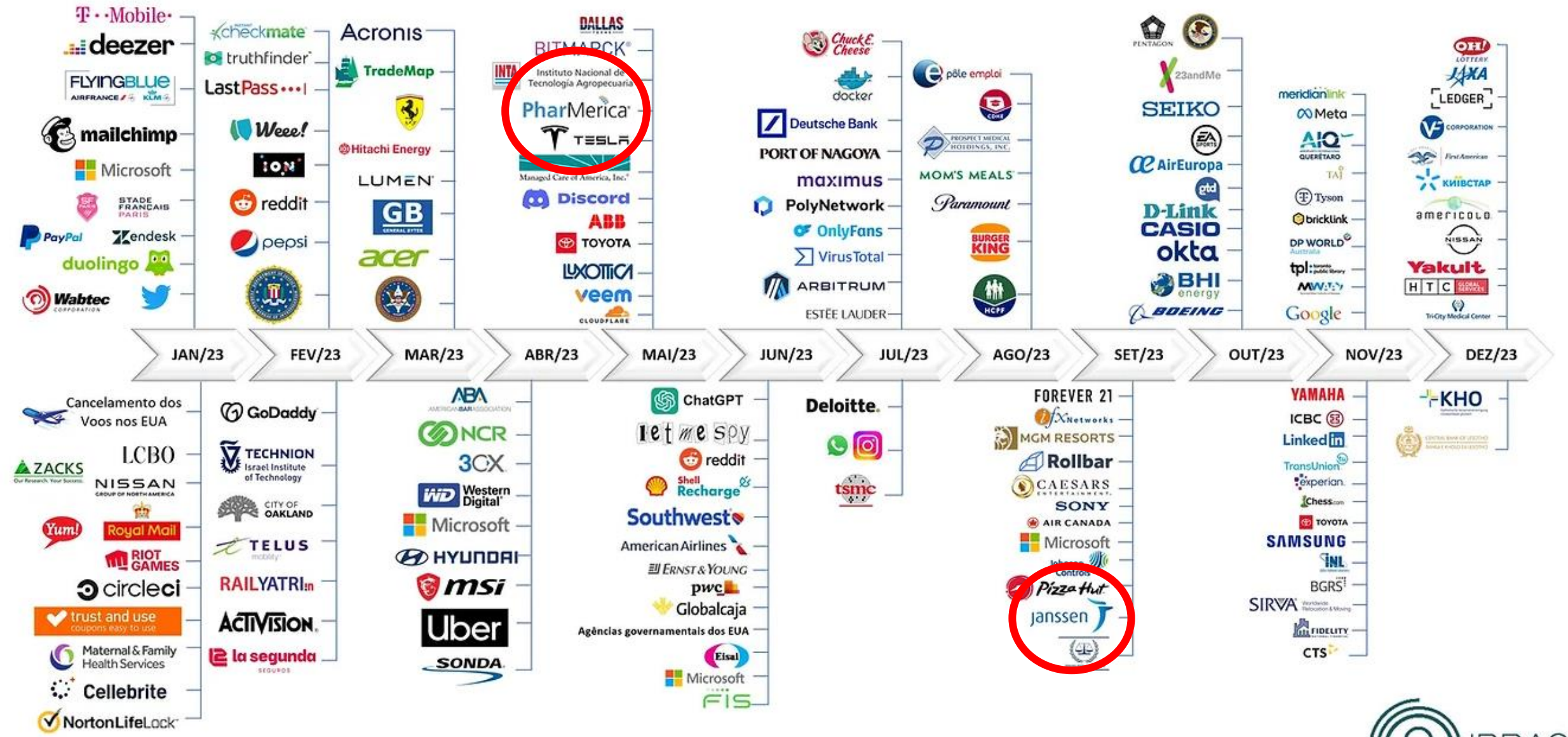
IBRASPD

Contexto Atual – Incidentes de segurança com repercussão na mídia*

- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

IBRASPD

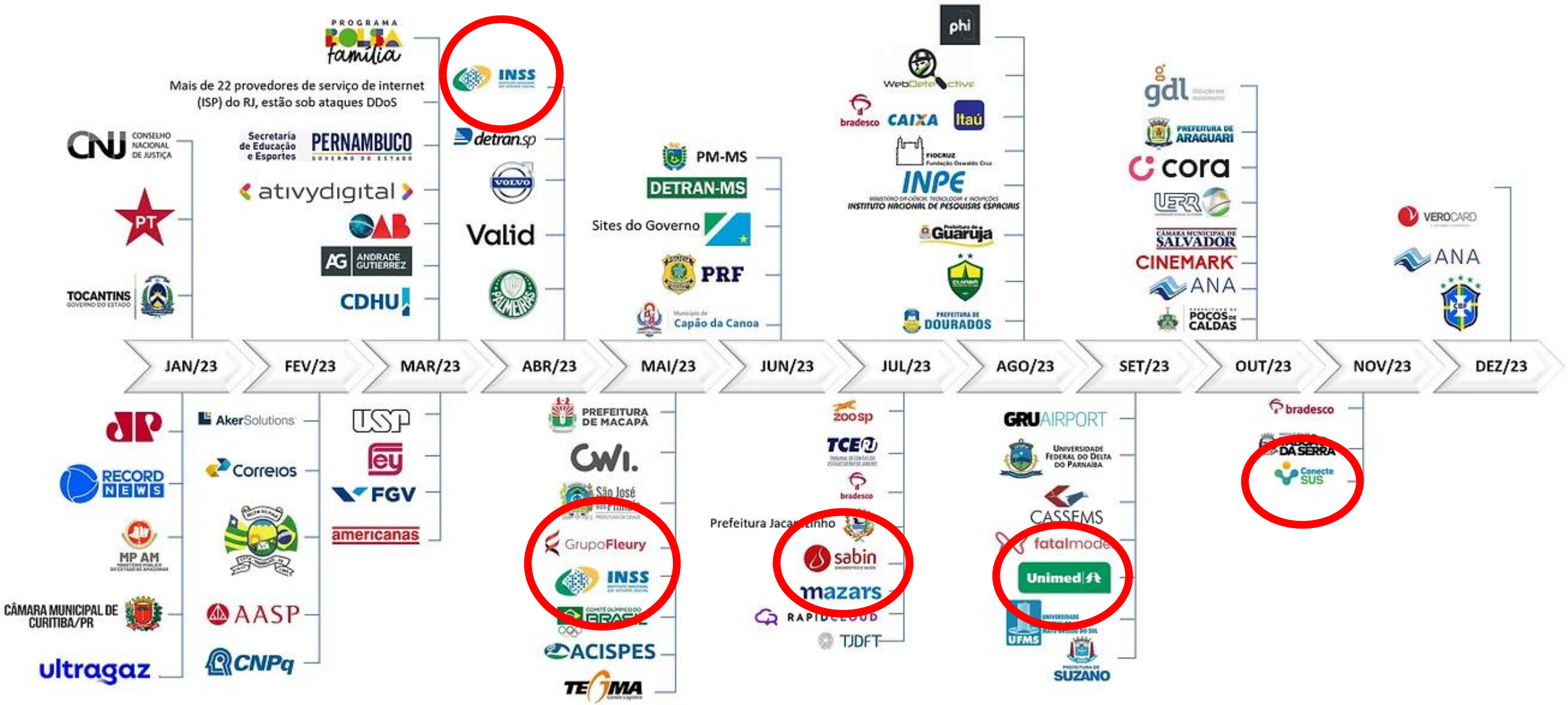
Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*



- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

IBRASPD

Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)*



- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

IBRASPD

NOSSOS HOSPITAIS ESTÃO EXPOSTO?

É LÓGICO QUE SIM!!! Não é se vai, mas quando!!!

- Foram mais de 100 bilhões de tentativas de ataques cibernéticos a empresas brasileiras nos últimos anos, como: **Phishing, Engenharia social, Malware, Ransomware, DDoS, outros**;
- Aproximadamente 4 ataques por segundo! Brasil ocupa a 2ª posição na América Latina;
- Somente de ataques de ransomware no Brasil são mais de 600 mil tentativas ao ano, sendo o 1º lugar na América Latina e o 4º no ranking global;
- FBI emitiu um alerta! Aumento de 33 % de ataques cibernéticos direcionados a dispositivos médicos;

Fontes: Forbes(2023); CISA Report (2023); Harvard Business Review (2023); ESET Security Report (2023); FortiGuard Labs (2024); Tiinside (2024)

HÁ 20 ANOS ATRÁS

Antigamente, um firewall e um antivírus eram considerados suficientes para a proteção das empresas por algumas razões:

- **Menos sofisticação nos ataques** (limitavam a vírus, worms e ataques de negação de serviço (DDoS))
- **Menor conectividade** (as redes empresariais eram menos interconectadas e a internet era menos onipresente)
- **Menos dispositivos** (não tínhamos tantos smartphones, tablets e dispositivos IoT (Internet das Coisas))
- **Foco principal nos endpoints** (computadores eram os principais dispositivos conectados às redes)

E HOJE ?

Hospitais modernos possuem múltiplos ATIVOS interconectados!!!

- Endpoints;
- Smartphones e Tablets;
- Integrações e API's,

  2023, 29% dos ciberataques tiveram as APIs como alvo principal; (Tlinside);
- Dispositivos Médicos,

  2023, 53% de todos os dispositivos médicos possuem vulnerabilidade entre eles bombas de infusão, marcapassos e monitores de pacientes; (FBI – IC3);
- Sistemas especialistas...

TENDENCIAS PARA 2024 ?

CONTINUARÁ EM EVIDÊNCIA O RANSOMWARE DIRECIONAL!!!

- As técnicas são as mesmas;
- O que muda são as táticas (Go Big or Go Home);
- Pela motivação Financeira (Segmentos indispensáveis ou primários a vida);
- Vendas de credenciais.

Fontes: FortiGuard Labs (2024)

TENDENCIAS PARA 2024 ?

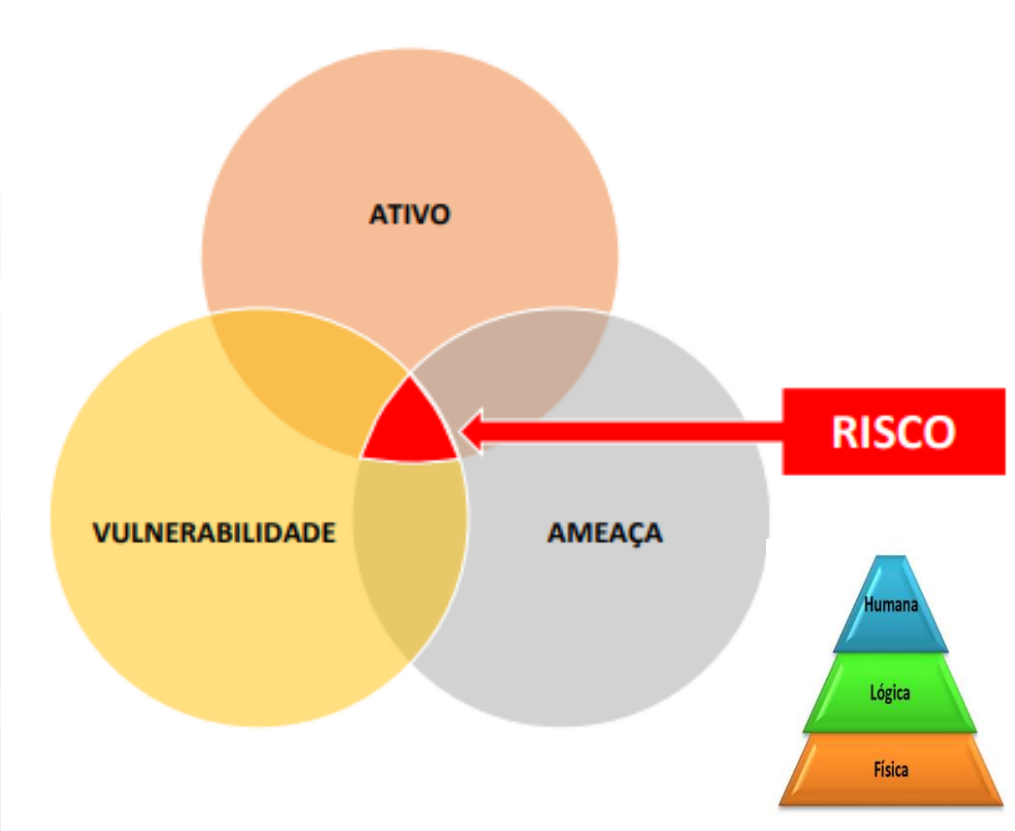
ZERO DAY !!!!

- Exploração de uma nova vulnerabilidade encontrada em sistemas;
- Vendas de credenciais.

Fontes: FortiGuard Labs (2024)

QUAIS PREVISÕES PARA 2024?

Hospitais modernos possuem múltiplos ATIVOS interconectados!!!
Riscos aumentados!!!



- Equipamentos de Imagem. Ex: Tomografia;
- Laboratórios. Ex: Terceiros;
- Integrações e API's. Ex: TISS
- Dispositivos Médicos. Ex: Robôs, bombas de infusão, marcapassos e monitores de pacientes;
- Sistemas especialistas. Ex: Semáforos.

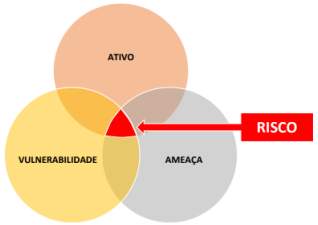
ATAQUE CIBERNÉTICO: INCIDENTES REAIS

Ciclo de vida de um incidente

Plano de Continuidade do Negócio

Plano de Recuperação de Desastres

Risco → Incidente → Dano → Recuperação



Redução

Prevenção

Detecção
55 dias

Repressão

Correção

Avaliação

EDR; IDS/IPS; SOE; IAM; RBAC; NAS; DLP; CASB; SOAR; SIEM; SOC

CUIDADOS À SEREM TOMADOS

NO EIXO DANO E RECUPERAÇÃO

- 91% das organizações pagaram pelos resgates (Capacidade de Resiliência);
- 29% delas o fizeram mais de uma vez;
- 23% das empresas brasileiras relataram perdas financeiras (Velocidade correção);
- 58% das empresas brasileiras sofreram uma tentativa de ransomware em 2022;
- 46% dos casos sendo bem-sucedidos para os hackers (Azar ou Excesso de Riscos);
- 92% tinham uma apólice de seguro para cyber ataques .

Fonte: Forbes (2023)

CONCLUSÃO

Adoção de práticas de segurança

- Implementação de medidas de segurança em dispositivos IoT;
- Atualização regular de sistemas e softwares com patches de segurança;
- Educação e treinamento de profissionais de saúde sobre cibersegurança;
- Investimento em soluções de detecção e resposta a incidentes (EDR);
- Consciência que os riscos são crescentes de ataques cibernéticos para hospitais, e, empresas que possuem um CISO são diferenciadas;
- Importância de medidas preventivas e de mitigação por soluções aderentes as vulnerabilidades do hospital;
- Necessidade de colaboração entre setores de saúde e cibersegurança;

YOUR FILES ARE ENCRYPTED

Your photos, documents and other important files have been encrypted with unique key, generated for this computer.

NEXT

Your network was compromised.

Important files on **your network** was **downloaded** and **encrypted**.
Our custom **Decrypt App** is capable of **restoring** your **files**.
In order to buy it you have to follow **Instructions** below. If you have questions please feel free to use **Live-Chat**.
Act quickly to get a **Discount**!

Decrypt App Price

You have **4 days, 17:03:03** until:

- **Decrypt App** special discount period will be discontinued.
- **Discount Price** is available until **10/15/22, 1:56 PM**

Discount Price: **$5000000**

Full Price: **$7000000**

Status

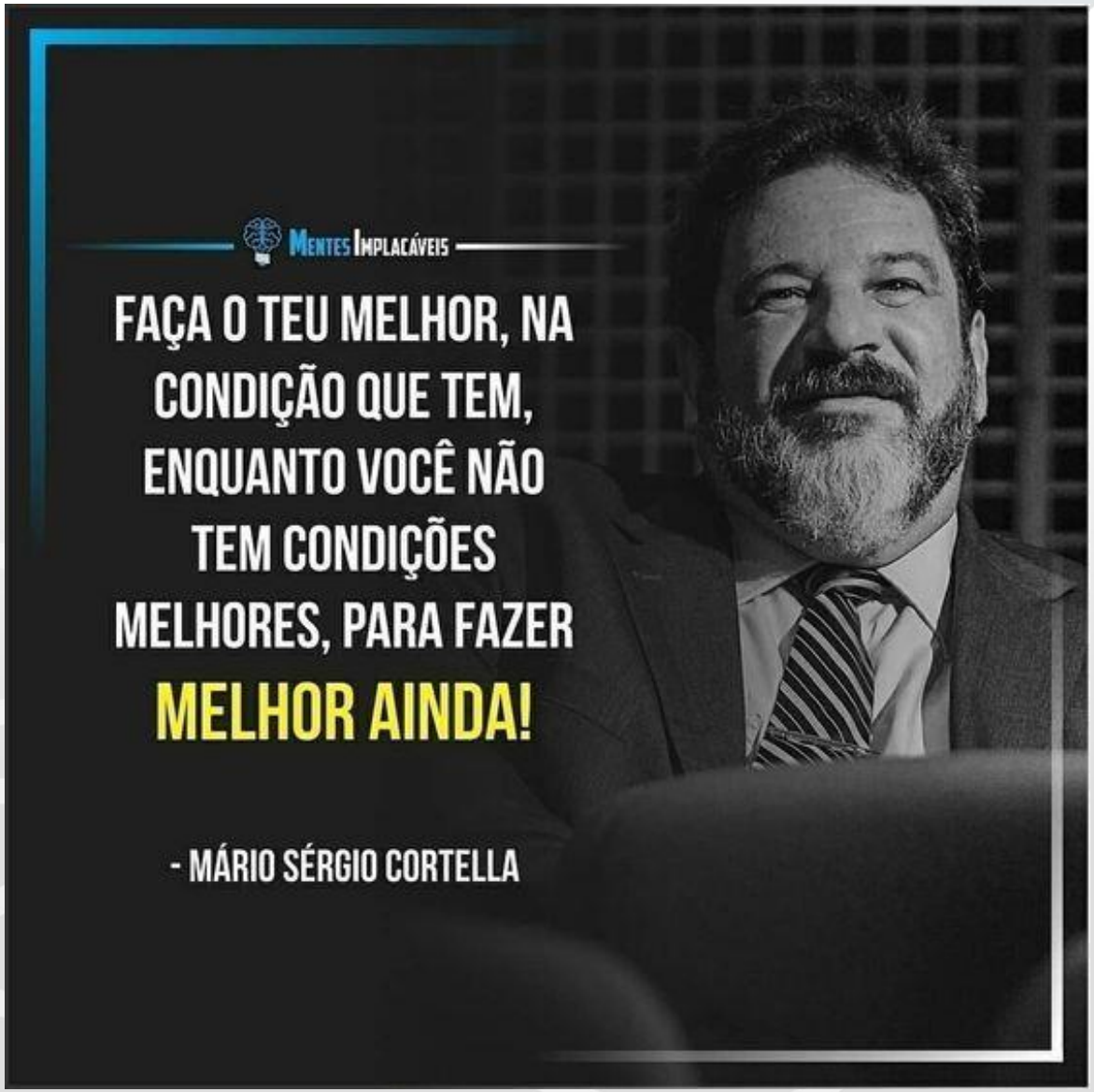
Awaiting payment of **$5000000** to one of the following wallets:

$5750000 (?) = 299.106064 BTC

$5000000 = 34307.671196 XMR

Instructions | Live-Chat | Trial Decrypt | Intermediary

Dúvidas


MENTES IMPLACÁVEIS
FAÇA O TEU MELHOR, NA CONDIÇÃO QUE TEM, ENQUANTO VOCÊ NÃO TEM CONDIÇÕES MELHORES, PARA FAZER
MELHOR AINDA!
- MÁRIO SÉRGIO CORTELLA

OBRIGADO!

Glaucio Erlei de Souza

Contato: dir.planejamento@hnsg.org.br