RMVALE TI 2021

Painel Segurança Cibernética em IoT

Alexandre Pinheiro

Diretor de Cyber Security e Inovação

grupo energy 20 anos telecom

INSTITUTO CTEM+

22/junho/2021

QUEM SOU EU?

Diretor de CyberSecurity, Inovação e Educação do Grupo Energy Telecom. Tem +25 anos de experiência na área de TIC. Contabilista e Bacharel em Sistemas de Informação. Especialista em Computação Forense e Perícia Digital pelo IPOG e MBA em Segurança Cibernética pela UNIFOR.

Possui diversas certificações na área de TIC e Segurança Cibernética como CompTIA CASP+, CompTIA CySA+, Google Professional Cloud Architect, Checkpoint CCSA e EXIN DPO (GDPR/LGPD) onde também é instrutor. **Possui as certificações ICS CISA (USA Gov) de proteção de infraestruturas críticas.**

Como Diretor do Grupo Energy Telecom, representa o grupo nas reuniões da NATO/OTAN no Cyber Academia and Innovation Hub na União Européia, onde o Grupo é membro colaborador.

Participou ativamente da edificação do CDTIC-Ciber no Pqtec, que o Centro de Desenvolvimento Tecnológico para P&D nas áreas de TIC e Segurança Cibernética, dentro do Parque Tecnológico São José dos Campos-SP.

É membro das entidades/instituições:

- OAB-SP (Comitê de Privacidade e Proteção de Dados)
- CRC-CE (Conselho Regional de Contabilidade do Ceará)
- APECOF (Associação Nacional dos Peritos em Computação Forense)
- CSA (Cloud Security Alliance)
- HTCIA (High Technology Crime Investigation Association)
- ISSA (Information Systems Security Association)
- Instituto CTEM+ (Membro Fundador), como Dir de Pesquisa, Ciência, Tecnologia e Inovação
- HDI Brasil, Membro do Board da HDI capítulo Norte/Nordeste
- CRA-CE (Grupo de Excelência em Defesa e Segurança)
- Instituto Iracema Digital do Ceará (Membro Fundador)
- IAPP (International Association of Privacy Professionals)

Professor convidado da disciplina de Defesa Cibernética da pós-graduação de Geopolítica e Relações Internacionais da ADESG-CE e IBEE-MT, e também professor de pós-graduação da Unichristus e UNIFOR.

DISCLAIMER

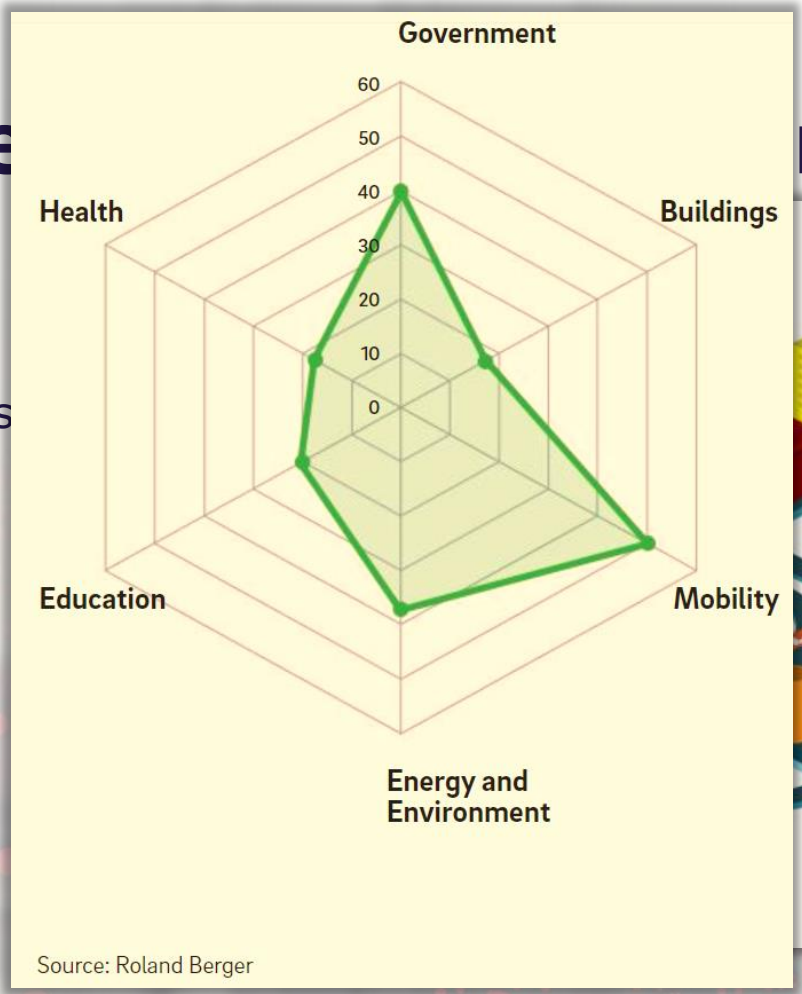
O conteúdo desta apresentação representa a opinião do palestrante, baseada na experiência e estudo das mais diversas fontes pesquisadas pelo mesmo.

A bibliografia utilizada para produção da apresentação, pode ser disponibilizada junto com os slides.

IoT
x
SEGURANÇA CIBERNÉTICA

Projeto de nte

- Governo Digital
- Saúde
- Educação
- Prédios inteligentes
- Mobilidade
- Energia
- Meio-Ambiente



Infraestruturas Críticas

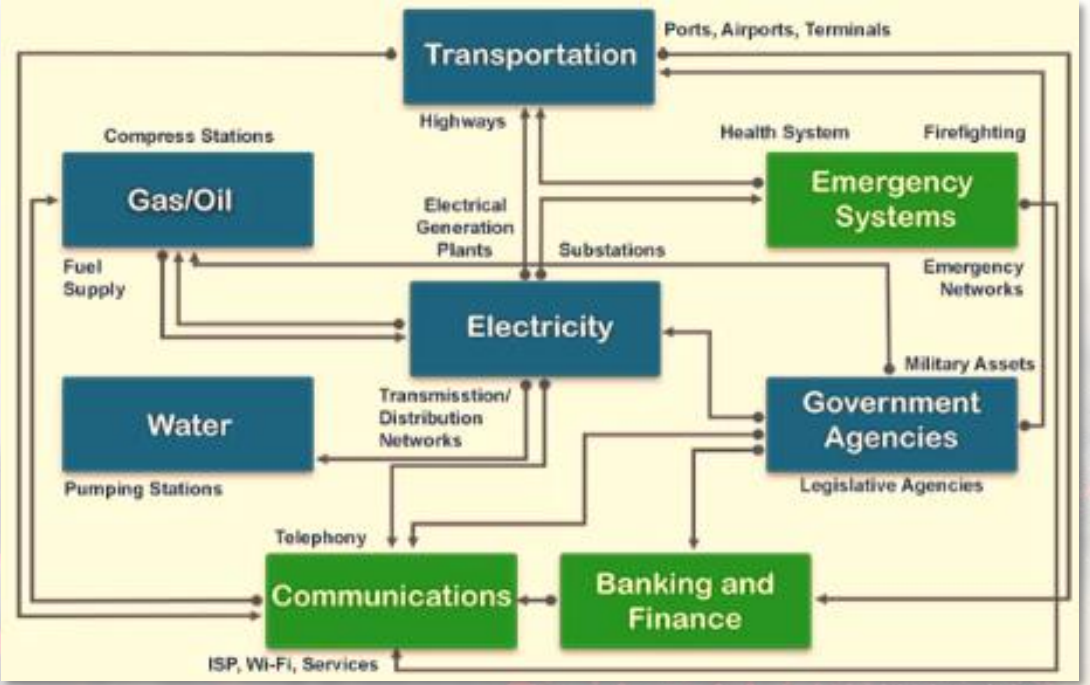
Componentes essenciais para a manutenção das funções vitais da sociedade, quanto à saúde, segurança e bem-estar.

- Sistema de Transporte
- Sistema de Comunicação
- Energia
- Água
- Bancos
- Etc

Fonte: Política Nacional de Defesa e a Estratégia Nacional de Defesa


Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Water and Wastewater
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
U.S. DEPARTMENT OF HOMELAND SECURITY
Homeland Security
Emergency Services
Transportation Systems
Energy
Nuclear
Information Technology
Healthcare and Public Health
Government Facilities
Food and Agriculture
Financial Services

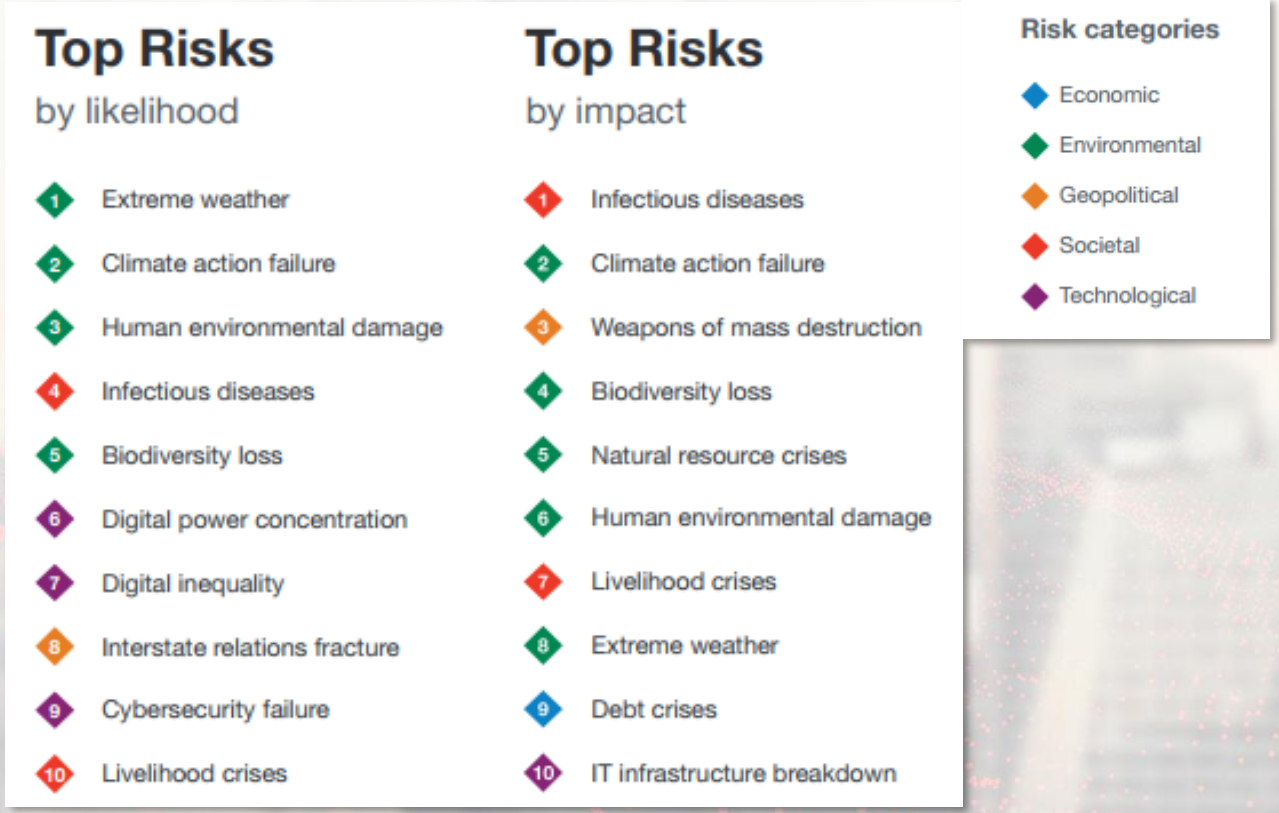
IC são interdependentes



Fonte: CISA

Tendência

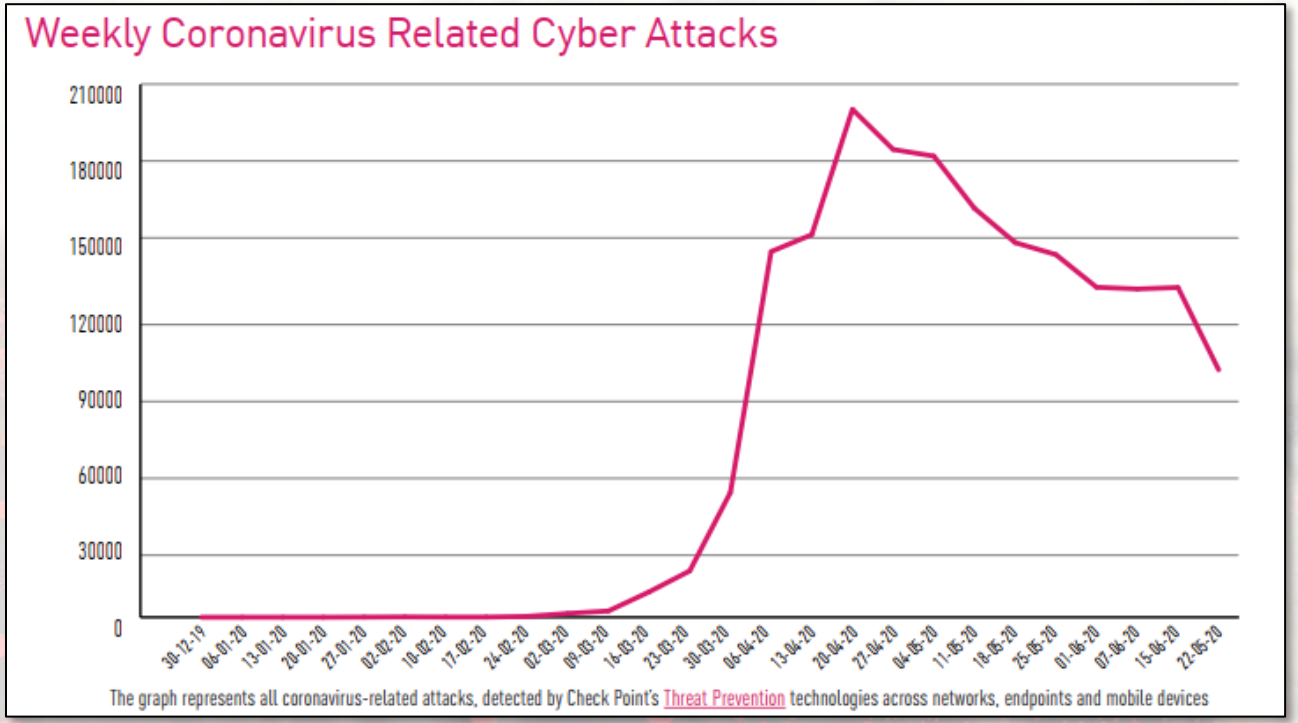
Fonte: Global Risk Report, Fórum Econômico Mundial, 2021



Ainda mais dependentes

- Transformação Digital
- “Datificação” (muito mais dados)
- + Eficiência

E a pandemia (COVID-19)?



Fonte: Cyber Attacks trend, Check Point research 2020 mid-year

E a Privacidade dos Dados?

- LAI, Lei nº 12.527/2011
- Carolina Dieckmann, Lei nº 12.737/2012
- Marco Civil, Lei nº 12.965/2014
- LGPD, Lei nº 13.709/2018
- ...

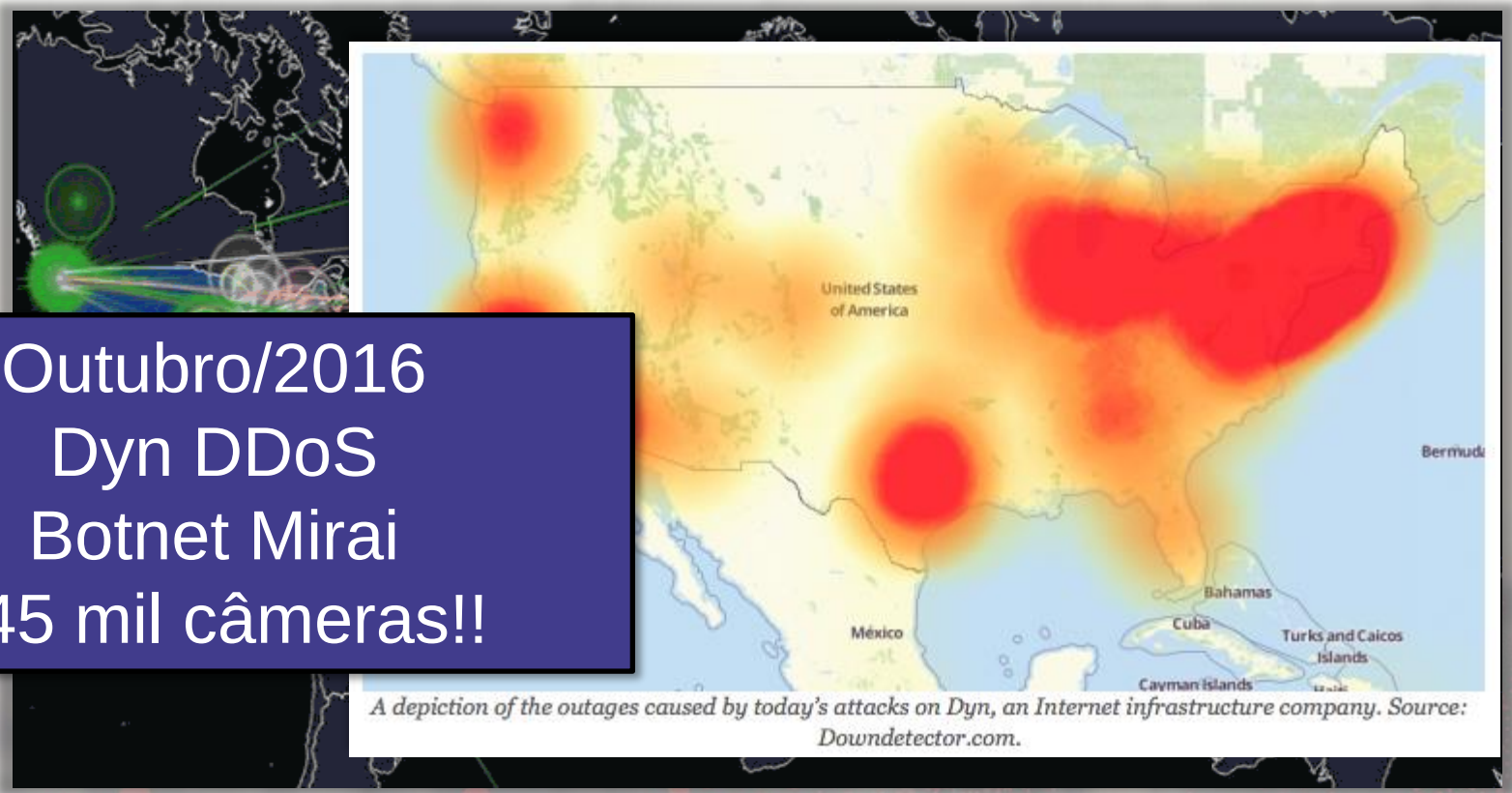
Vazou, mas não fui atacado!

- ENQUADRAMENTO NA LGPD INDEPENDE DE INVASÃO
- INVASÃO TEM TIPIFICAÇÃO PRÓPRIA (Art. nº154-A CP)

> *"Art 154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita."*
>
> Art nº154-A CP


Quais as chances de ...?

IoT?



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

Outubro/2016
Dyn DDoS
Botnet Mirai
145 mil câmeras!!

Cas

EDITORS' PICK | 7,839 views | Apr 8, 2020, 07:08am EDT

Cyber Attacks Against Hospitals Have 'Significantly Increased' As Hackers Seek To Maximize Profits

Davey Winder Senior Contributor ⓘ

Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

Cas

SECRETARIA DA FAZENDA
Governo do Estado do Ceará

Institucional
Nossa história e estrutura organizacional

Contencioso
Processos, pautas de julgamento

Serviços
Sistemas e aplicativos on-line

Finanças Públicas
Balanço geral, tabelas e índices financeiros

Legislação Tributária
Leis e parâmetros jurídicos

- Institucional
- Contencioso
- Sua Nota Vale Dinheiro
- Educação Fiscal
- Comunicação
- Serviços Online
- Finanças Públicas
- Legislação Tributária
- Informações Gerais
- Fale Conosco
- Acesso a Informação
- Perguntas Frequentes

Órgãos Vinculados
JUCEC
Portal do Governo
OK

Acesso Rápido
DO QUE VOCÊ PRECISA?

VOLTAR IMPRIMIR

Comunicado - 12.05.2017

ATENÇÃO !!!

Senhores usuários,

Em decorrência de um ataque cibernético chamado Wanna Cry, a SEFAZ-CE decidiu retirar temporariamente do ar os serviços abaixo:

1. Legislação tributária: http://legs.sefaz.ce.gov.br;
2. Recebimento de arquivos via SefazNet;
3. Recebimento de arquivos do SPED;

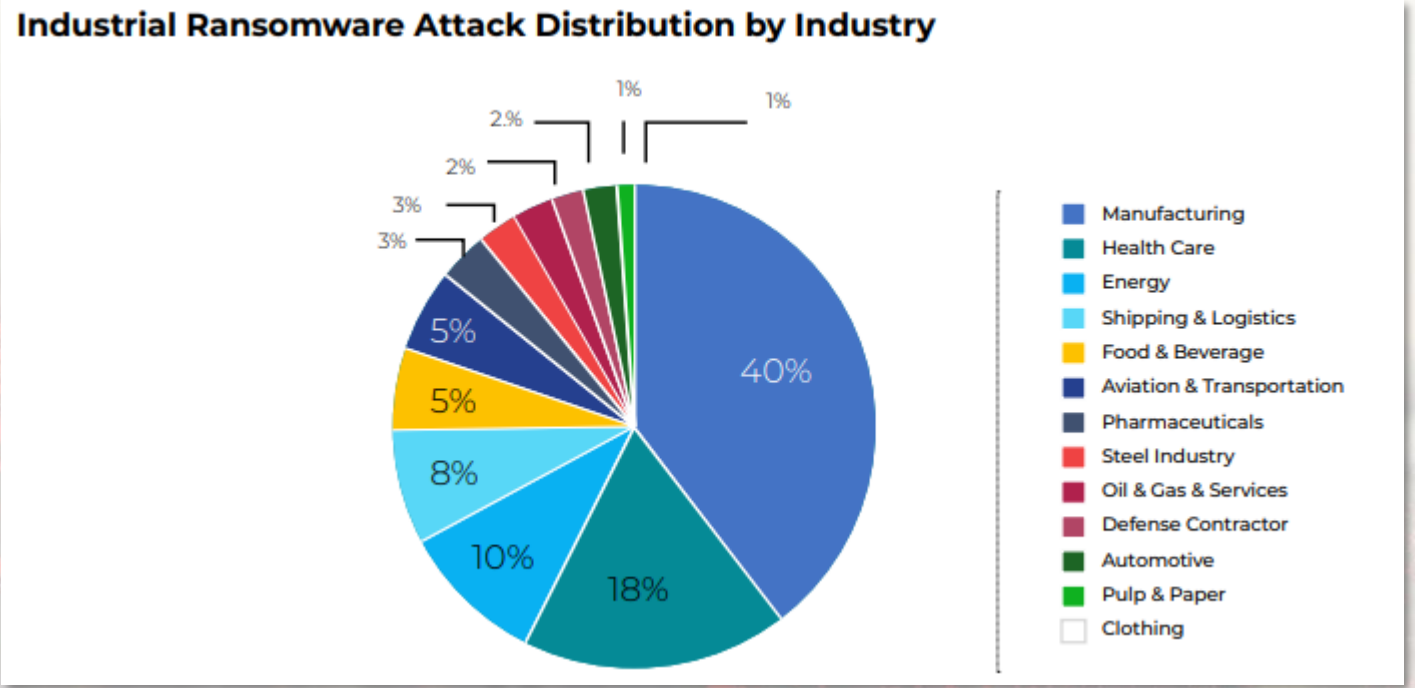
Assim que a SEFAZ-CE estiver segura contra o referido ataque, os serviços acima serão reestabelecidos.

Pedimos desculpas pelos transtornos e contamos com a compreensão de todos.

Atenciosamente,

Coordenadoria de Tecnologia de Informação da SEFAZ-CE

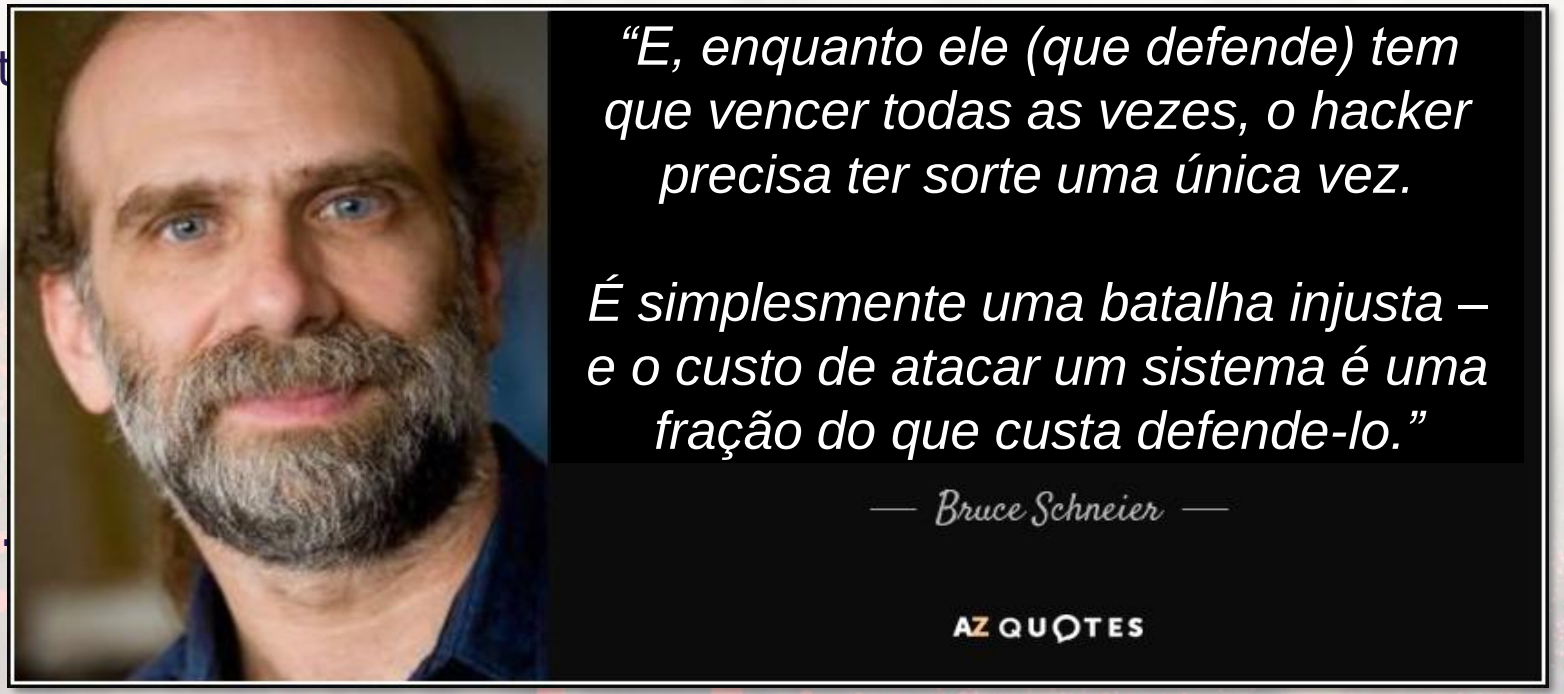
Ransomware em ICS de 2020



Fonte: OTORIO

Disputa injusta

- At
- A
- O
- 2
- …



Desafios adicionais

- 5G
- Fim do IPV4
- Falta de profissionais
- ...

~~IPV4~~ => IPV6

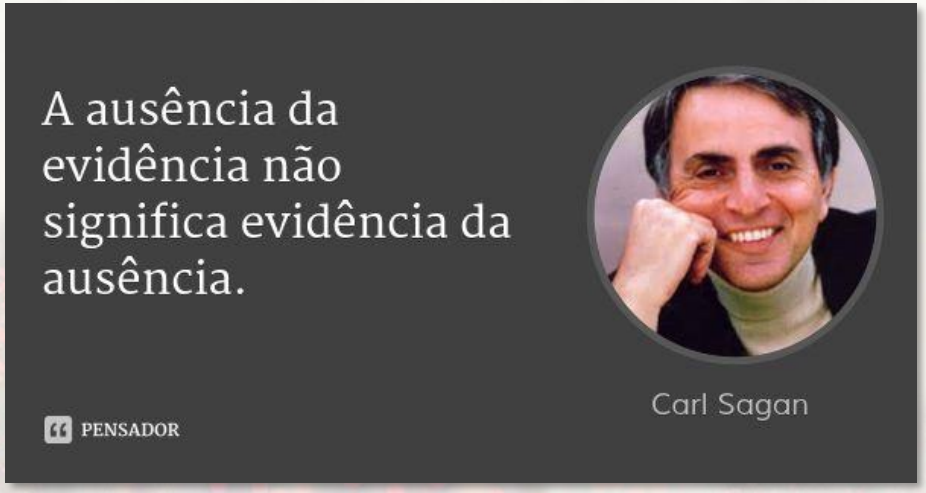
Itens essenciais em Projetos de IoT

1. Comunicação
2. Cloud
3. Segurança Cibernética

Investir nas 3 frentes

Uma estratégia eficiente e orquestrada de gestão de incidentes pode diminuir em até 80% o tempo de solução de um ataque.

Não existe segurança 100%!



NOC + SOC + CyberRange

- Monitoramento 24x7
- Visibilidade
- Proatividade
- Resposta a Incidentes
- Capacitação continuada
- Compliance

Contatos

Alexandre Pinheiro

alexandre.pinheiro@energytelecom.com.br

+55 (85) 3533-5800 / (85) 99263-3642

pinheiroalexandre

grupo energy telecom

www.energytelecom.com.br

INSTITUTO CTEM+

www.ctemmais.org