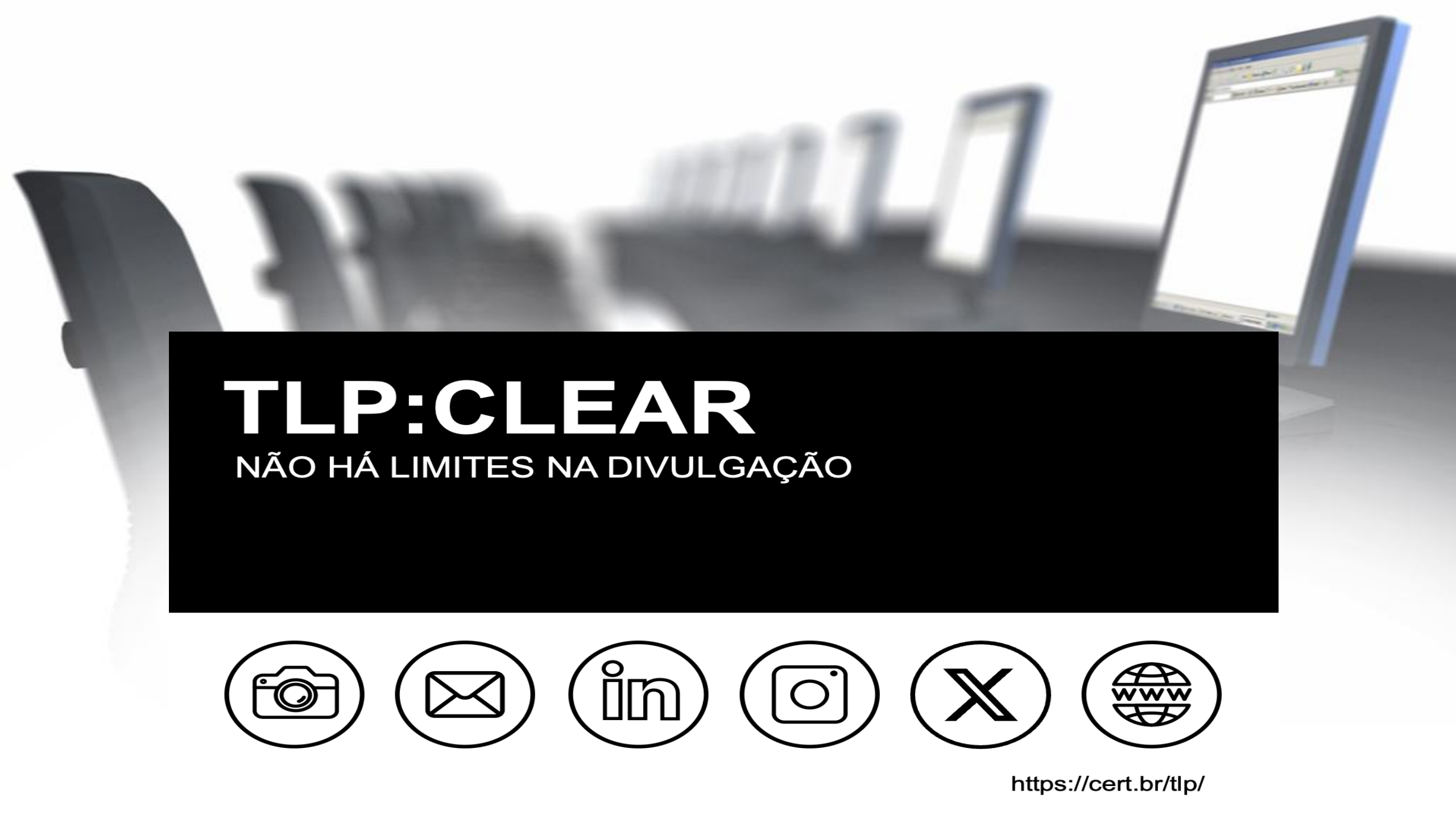

TLP:CLEAR

NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

INVESTIR EM EDUCAÇÃO

Sugestões para a Segurança da Informação & I.A. para Pequenas e Médias Empresas Brasileiras

EST. 2021

RedZone

Quem somos

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

Fernando Amatte

Cybersecurity Specialist

CISSP - Certified Information System Security Professional

Alexandre Armellini

Cybersecurity Specialist

CISSP - Certified Information System Security Professional

- Somam mais de 50 anos de experiencia atuando na área de Segurança da Informação e Segurança Cibernética, para empresas de todo segmento pelo mundo. Fundadores do programa **Red Zone** e outras iniciativas voltadas para **EDUCAÇÃO** amparando indivíduos e apoiando empresas.

RedZone

CYBER GURUS

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

O Cenário

- **Brasil**
  - **Ataques a cada 16 segundos (“Mundo 11”)**
- **Criminosos**
  - **Extremamente PROATIVOS**
  - **50% dos ataques usam IA**
- **Defesas**
  - **93% das empresas dizem já usar IA para detecções**
  - **5% são eficazes**
- **Grande Déficit em Segurança da Informação**
  - **Extremamente Reativos**
  - **Investem errado**
  - **Negócios realizados sem amparo técnico**
  - **Custos elevados por violação (1,5 Milhão US$)**
  - **Extrema exposição**
  - **Ambientes depreciados (EOL)**
  - **Falta de atualizações (Patches)**
  - **Dificuldade em automação**
  - **Falta de profissional capacitado (+/- 500k déficit)**

Fonte: Sophos & Forescout

EST. 2021
RedZone

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

Os Desafios

- **40% do mercado subestima IA nos ataques**
- **Falta de profissionais capacitados**
- **Investimentos em cibersegurança**
  - **Brasil 12º no mundo**
  - **Previsão de 21,6 bilhões em 2025**
  - **Promessa de 105 bilhões até 2028**
- **Investimentos em IA**
  - **150 Bilhões em 2025**
    - **Detecção Ruim**
    - **Automação de CSIRT incompleta**
    - **Análise de Risco errada**
    - **Phishing & Ransomware (Eng. Social)**
    - **Shadow IA (Falta de know-how & monitoramento)**
- **Investimentos em Educação**
  - **Capacitação HDB - 33 Milhões**
  - **Empresas privadas – 450 Milhões**

EST. 2021
RedZone

Fonte: INCC, ClearSale & Forescout

2024 -> 2025

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

- **Análises dos últimos 12 meses do BRASIL**
  - **Ransomware (Sophos)**
  - **Violação de Dados (INCC)**
  - **Fraudes (Apura, ClearSale & Crowdstrike)**
  - **Detecção (SANS)**
- O que Fazer?
- Pequenas e Médias Empresas (INCC)
- Conclusões

RedZone
EST. 2021

Ransomware

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

- 32% dos incidentes são vulnerabilidades conhecidas
- 40,2% das vítimas tem falta de expertise
- 40,1% falhas desconhecidas da organização
- A falta de pessoas *(“braço”)*, contribuiu para 39,4% dos ataques
- 50% puderam usar Backup para voltar a ativa
- Tempo OFF => 37% (1 semana) e 28% (1 mês)

- **49% das vítimas pagaram os resgates!!!**

Fonte: Sophos

RedZone
EST. 2021

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

Violação de Dados

- 50% das empresas relataram perda de dados em 2024
- Malwares (e Ransomware) disfarçados de atualizações de software no topo da lista de ameaças
- Foco principal dos investimentos tem sido a proteção contra vazamentos de dados e IA (ou ambos)
- **Custo médio por violação: R$ 33.53 milhões**
- Custo estimado de **R$ 1.545** por registro violado
- **Perda de empregos:** A cada violação, **74 empregos são eliminados**
- **Impacto em Renda (massa salarial):** Cada ataque reduz **R$ 26 milhões da renda brasileira**

Fonte: INCC

EST. 2021
RedZone

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

Fraudes

- Considerando que:
  - **22 minutos entre uma POC e sua exploração**
  - **Contágio entre hosts => 48”** em média
- 26% erros de exposição em nuvem
- 52% por credenciais expostas
- 79% usam engenharia social
- 98% dos casos usam IA
- 150% de crescimento de mídias sociais (caos)
- SUDESTE o mais explorado (população)
- Mais usados são Whatsapp, Facebook e Telegram

RedZone EST. 2021

Fonte: Apura, ClearSale & Crowdstrike

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

Detecção

- SOC
  - **30% são terceirizados**
  - **79% trabalham 24x7**
  - **42% usam AI/ML sem CUSTOMIZAÇÃO (out of the box)**
  - **16.8% não sabem dizer se usam IA**
  - **43% dependem do SIEM e são limitados à SIEM (TOP SKILL)**
  - **85% dependem de alertas dos End-Points**
  - **69% usam processos manuais para obter métricas**
  - **73% trabalham remotamente**
  - **62% reclamam da empresa**
- Baixo custo e conhecimento limitado à ferramentas
- Empresas não cumprem promessas de retenção

Fonte: Pesquisa SANS

EST. 2021
RedZone

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

O que Fazer?

- **Need To Know**
  - **50% de dispositivos vulneráveis são ROUTERS**
  - **Mais visados: OT, IOT e Dispositivos Médicos (IOMT)**
  - **Acesso remoto, FTP e TELNET em uso abundante**
  - **Novidades: 12 novos equipamentos só em 2025**
  - **OT (gateways universais, senhas padrão e acesso físico)**
  - **IOT (Impressoras, Broadcasters, Telemidia, Equipo Industrial)**
  - **IOMT (Exames Laboratoriais, Pontos de Acesso, Diálise....)**
  - **+ de 50% usam Win10 (Suporte acaba em Ago/25)**
  - **E ainda temos Windows mais antigos pelo Brasil**
    - **2,7% em Governos**
    - **2,2% em Saúde**
    - **1,8% em Fábricas**

EST. 2021
RedZone

Fonte: Forescout

O que fazer?

- **Need To Do**
  - **Não foque somente em IA**
  - **Não trate IT, OT, IOT e IOMT isoladamente (risco)**
  - **Evite soluções únicas**
  - **Aplique SEGMENTAÇÃO**
  - **Atualize máquinas Windows (considere extensão de suporte com a MS)**
  - **Consulte especialistas técnicos e não apenas comerciais**
  - **Entenda RISCOS de TI ao negócio e vice-versa**

RedZone
EST. 2021

Fonte: Forescout

PMEs (Pequenas e Médias Empresas)

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO
https://cert.br/tlp/

- É a HORA de MUDANÇAS
  - Constituem a base da economia brasileira.
  - Contribuem com 30% do PIB.
  - Geram 62% dos empregos formais.
  - A maioria carece de recursos técnicos, financeiros e orientação
  - 81% dessas empresas têm 02 funcionários dedicados a cibersegurança
  - Se os Crimes Cibernéticos subirem 10% nos próximos 3 anos, impactarão o PIB em 1 Trilhão

  - **Se investirem 10% ao ano em segurança cibernética, só as PMEs teremos um retorno financeiro de 120 Bilhões nos próximos 3 anos.**

Fonte: INCC

RedZone
EST. 2021

TLP:CLEAR
NÃO HÁ LIMITES NA DIVULGAÇÃO

https://cert.br/tlp/

Conclusões

- Executivos precisam mudar investimentos e foco em TI
- ‘C’ Levels precisam de ajuda e rever conceitos.
- IA não é TUDO! Ajuda, mas não é o cálice sagrado!
- A falta de profissionais capacitados é clara.
- A **Educação** é necessária.
- Temos 55 milhões de brasileiros com mais de 60 anos.
- Onde investir nos brasileiros no futuro?
  - **25 Milhões estão no ensino fundamental**
  - **8 Milhões estão no ensino médio**
  - **10 Milhões estão nas faculdades**
  - **800 mil fazem exatas**
  - **Apenas 10% de exatas são ligadas à COMPUTAÇÃO.**

- **Governo e Empresas Privadas precisam fazer as contas!**

EST. 2021
RedZone

OBRIGADO

+55 19 99111-7486
+55 19 98124-0722
contato@redzonearea.com

EST. 2021

RedZone