CURSO
CIBERSEGURANÇA


tv jornal

Francisco Nauber Bernardo Gois
Dsc. Informática Aplicada

CGE | CONTROLADORIA E OUVIDORIA GERAL DO ESTADO
GOVERNO DO ESTADO DO CEARÁ

RBCIP pesquisa e inovação

Auditor de Controle Interno, Professor das Especializações em Ciência de Dados (UNIFOR) e Pesquisador associado da Rede Brasileira de Certificação, Pesquisa e Inovação - RBCIP

聖若瑟大學
UNIVERSITY OF SAINT JOSEPH

Pós Doutorado- Laboratório de Neurociência Aplicada (2022-2025)

Doutorado em Informática Aplicada (2012-2017)
Search-based Stress Test: an approach applying evolutionary algorithms and trajectory methods


A LONG TIME AGO
Fortaleza, Brazil
1987


A LONG TIME AGO
Fortaleza, Brazil
1987

CYBERSECURITY FUNDAMENTALS

CYBERSECURITY RESPONSIBILITY

Who is Responsible for Cybersecurity?

Cybersecurity is a shared responsibility.

Source : Homeland Security

Brasil concentra metade dos ataques de ransomware na América Latina, aponta Kaspersky

Relatório revela aumento de 12% no país, enquanto região registra queda geral; saúde, governo e empresas seguem como principais alvos.

Kaspersky: novo estudo mostra aumento das vítimas de ransomware no Brasil

21 de maio de 2025

Saúde, Financeiro e setor de serviços são os principais alvos dos ataques. Números destacam a necessidade de melhorar a prevenção, pois não há como remediar as perdas após um ataque.

Novo relatório da Kaspersky Digital Footprint Intelligence (DFI), que destaca as ameaças mais graves e proeminentes encontradas na dark web, revela um crescimento alarmante dos ataques de ransomware direcionado a empresas no Brasil. O estudo destaca um aumento de 69% nessa atividade no ano passado e demonstra a crescente sofisticação e frequência desses crimes.

O relatório mostra que, em 2024, o Brasil testemunhou um número alarmante de ataques de ransomware, que afetaram 105 organizações. Esse número representa uma escalada preocupante, considerando com os 62 casos em 2023 e os 39 em 2022. A situação é agravada pelo fato de haver nove empresas recorrentes, ou seja, que sofreram dois ataques no período de um ano.

Você tem *backup*?

Proteja-se de *ransomware* e preserve seus dados!

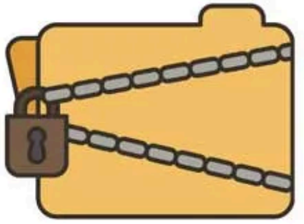
Attacker

Phishing email

Ransomware execution

Decryption key

Demand ransom

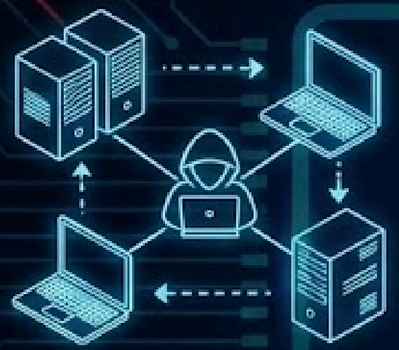


Data encryption

Expose files

1. RANSOMWARE (O MAIOR RISCO DO SETOR PÚBLICO)

ENTRADA:
Phishing +
Credenciais Vazadas

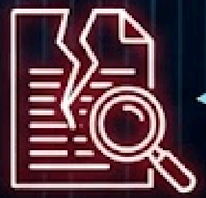


PROPAGAÇÃO:
Lateral Movement

IMPACTOS FINANCEIROS
(Saco de dinheiro com cifrão)

REPUTACIONAIS
(Ícone de reputação quebrada)

OPERACIONAIS
(Engrenagens paradas)



RELAÇÃO DIRETA COM FALHAS DE AUDITORIA


PORQUE TEM TANTO ATAQUE DE RANSOMWARE NO BRASIL?
Be Strong Cast
“Porque tem tanto
ataque de ransomware
no Brasil?
Watch on YouTube


FreedMine


BREAKING NEWS
VIVO
FALHA CIBERNÉTICA AFETA VOOS, BANCOS E SERVIÇOS MÉDICOS
Aeroportos dos EUA e Europa paralisaram operações
CNN BRASIL
08:41
youtube.com/@CNNBrasil
@CNNBrasil
APA
CNN NOVO DIA

O Auditor Contra a Ameaça Invisível

- Ransomware derrubando prefeituras, tribunais, assembleias, universidades.
- Perda de backups = prejuízo millionário + paralização de serviços.
- Auditoria tradicional não cobre riscos digitais modernos.

Exemplos para abrir (curtos e impactantes):

- Caso da Prefeitura de Recife: indisponibilidade por ataque.
- Caso do TJ-RS: paralisaçâo total e impacto em processos.
- Governo da Costa Rica: estado de emergência por ciberataque.

Frase de impacto: “*O problema não é se o órgão será* atacado.
É quando... e se ele estará preparado.”


MR. ROBOT

Frameworks que funcionam:

- **NIST CSF**
- **MITRE ATT&CK**
- **CIS Controls 1 a 6** (os que importam para a auditoria)

Check rápido que auditores podem aplicar:

1. Inventário de ativos?
2. Controle de acessos atualizado?
3. Backups testados?
4. Logs com retenção adequada?
5. Plano de continuidade revisado?
6. Patches de segurança aplicados regularmente?

Riscos prioritários para órgãos públicos:

- Exposição de sistemas legados
- Falta de MFA
- Backups online (criptografáveis)
- Dependência excessiva de fornecedores
- Falhas de compliance com LGPD

CIA (Confidencialidade, Integridade, Disponibilidade)
Ataques: phishing, ransomware, DDoS, insider threat supply chain
Vulnerabilidades mais comuns no setor público:

- Servidores expostos
- Credenciais vazadas
- Falta de MFA
- Backups inseguros

O que o auditor deve perguntar:

- Onde estão os ativos críticos?
- Quem administra privilégios?
- Existe MFA?
- Existe plano de continuidade documentado?
- Existe plano de segurança aprovada e atualizada Ja ?

CONCEITOS-CHAVE PARA AUDITORIA DE CIBERSEGURANÇA

CIA (A TRÍADE DA SEGURANÇA)

- **C:** Confidencialidade
- **I:** Integridade
- **A:** Disponibilidade

ATAQUES COMUNS

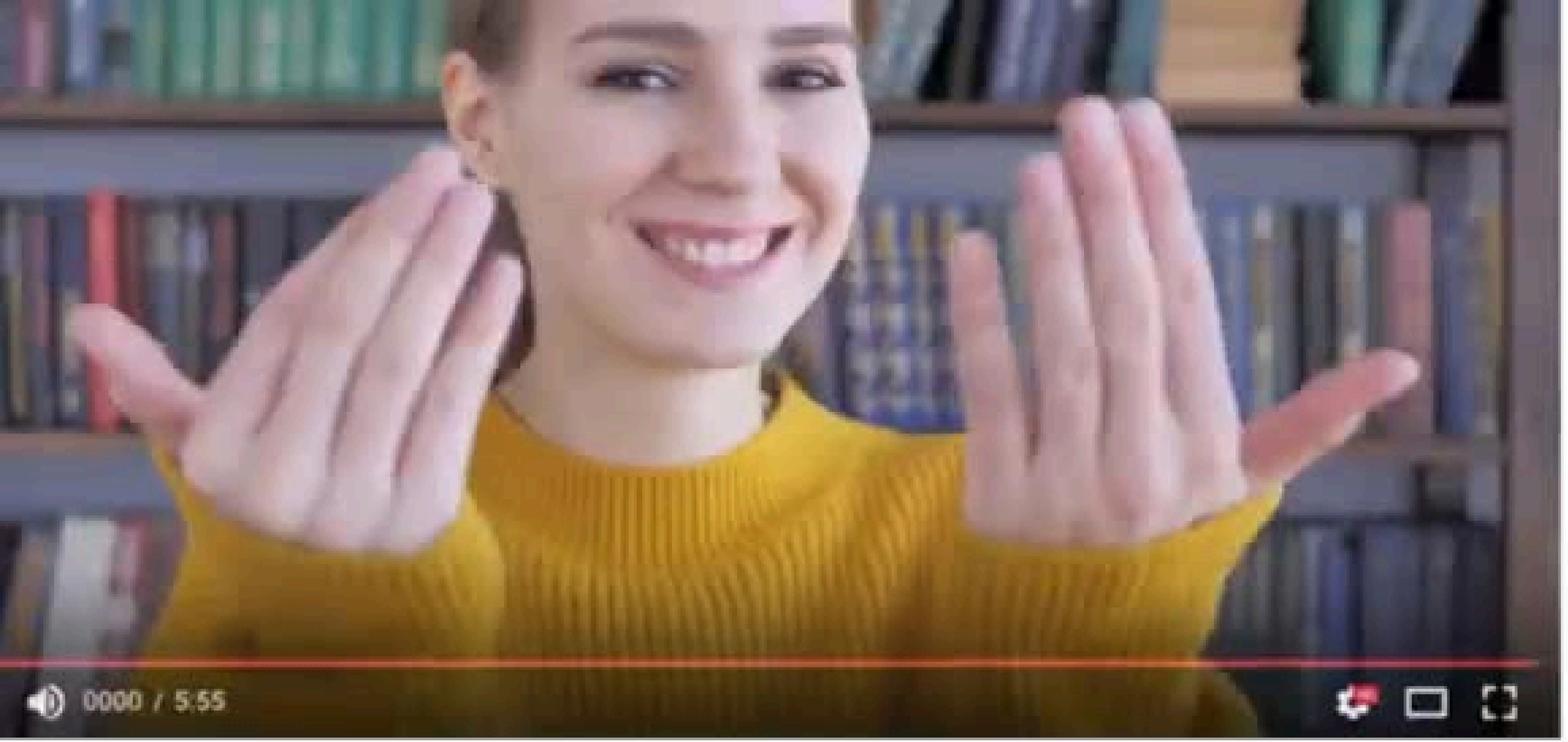
- Phishing
- Ransomware
- DDoS
- Insider Threat
- Supply Chain

VULNERABILIDADES PÚBLICAS

- Servidores expostos
- Credenciais vazadas
- Falta de MFA
- Backups inseguros
- Falta de segregação de funções

O QUE O AUDITOR DEVE PERGUNTAR

- Onde estão os ativos críticos?
- Quem administra privilégios?
- Existe MFA?
- Existe plano de continuidade documentado?
- Há política de segurança aprovada e atualizada?



ortes de PODCAST do Brasil

10 1 SHARE

INSCRITO


Soluções – Segundo Lugar
Trabalho: Fale com o orçamento
Autor: Francisco Nauber Bernardo Gois

CGE | CONTROLADORIA E OUVIDORIA GERAL DO ESTADO
GOVERNO DO ESTADO DO CEARÁ

USJ MACAO

RBCIP pesquisa e inovação

Utilização de agentes inteligentes na triagem de pacientes no sistema público de saúde

Tema: TRANSFORMAÇÃO DIGITAL PARA OS CIDADÃOS


USJ Laboratory of Applied Neurosciences
Copy link
Watch on YouTube


HOPE

francisco.gois@cge.ce.gov.br

Obrigado!!!

Obrigado!!!