Aspectos de segurança e comunicação de dados no Censo Agropecuário

Bruno César Barbosa Alves

Gerência Técnica de Telecomunicações

Diretoria de Informática DI

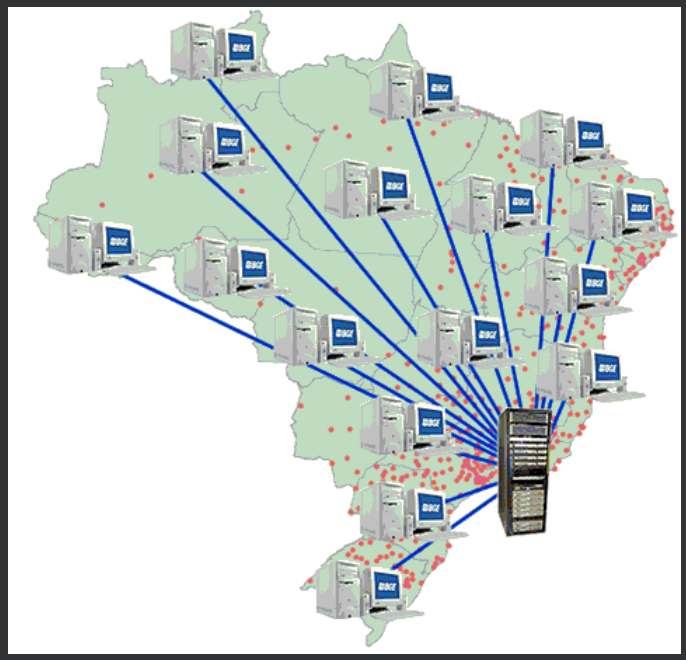
IBGE

Capilaridade da Rede do IBGE

- As pesquisas e o Censo digital realizado pelo IBGE são sustentados por uma infraestrutura de comunicação de capilaridade nacional
- Todos os dados coletados são transmitidos, de forma segura, através da Internet, para os datacenters localizados no Rio de Janeiro e São Paulo

É preciso prover comunicação entre:

- 27 Unidades Estaduais, uma em cada capital
- 600 agências, em diversos municípios, em todos os estados brasileiros
- 3 Datacenters (2 no Rio de Janeiro e 1 em São Paulo)
- Milhares de postos de coleta (em operações de censo)



Diversidade de Recursos

- Os recursos de comunicação utilizados são os mais diversos, por motivos como:
    - Limitações tecnológicas locais
    - Dificuldades de acesso físico (ex: Região Amazônica)
    - Necessidade de mobilidade
        - Uso de dados móveis (3G/4G)
        - Acesso móvel por satélite (BGAN)
- Exemplos de tecnologias de telecomunicação utilizadas:
    - Nas Unidades Estaduais e Datacenters
        - Acesso à Internet, circuitos ponto a ponto (fibra ótica) e MPLS
    - Nas agências
        - xDSL, fibra ótica, rádio digital, dados móveis (3G/4G), antena satelital fixa (VSAT), antena satelital móvel (BGAN)

Diversidade de Recursos

Segurança da Informação no IBGE

- O IBGE coleta, armazena, processa, analisa e disponibiliza grande quantidade de dados e informações
  - A segurança da informação precisa ser garantida
    - A **confidencialidade** dos dados coletados é um dever do Instituto
    - A **disponibilidade** das informações publicadas é fundamental
    - A **integridade** dos dados precisa ser mantida para que os resultados das pesquisas sejam de alta confiabilidade

Segurança da Informação no IBGE

As informações do IBGE despertam muito interesse, inclusive de hackers

Segurança em Profundidade

Instrumentos de Proteção

- Os Controles de Segurança são de diversas naturezas:
  - Administrativa
  - Técnica
  - Gestão
  - Legal

Política da Segurança da Informação e Comunicações do IBGE

POSIC 2017/2018

Segurança da Informação
e Comunicações

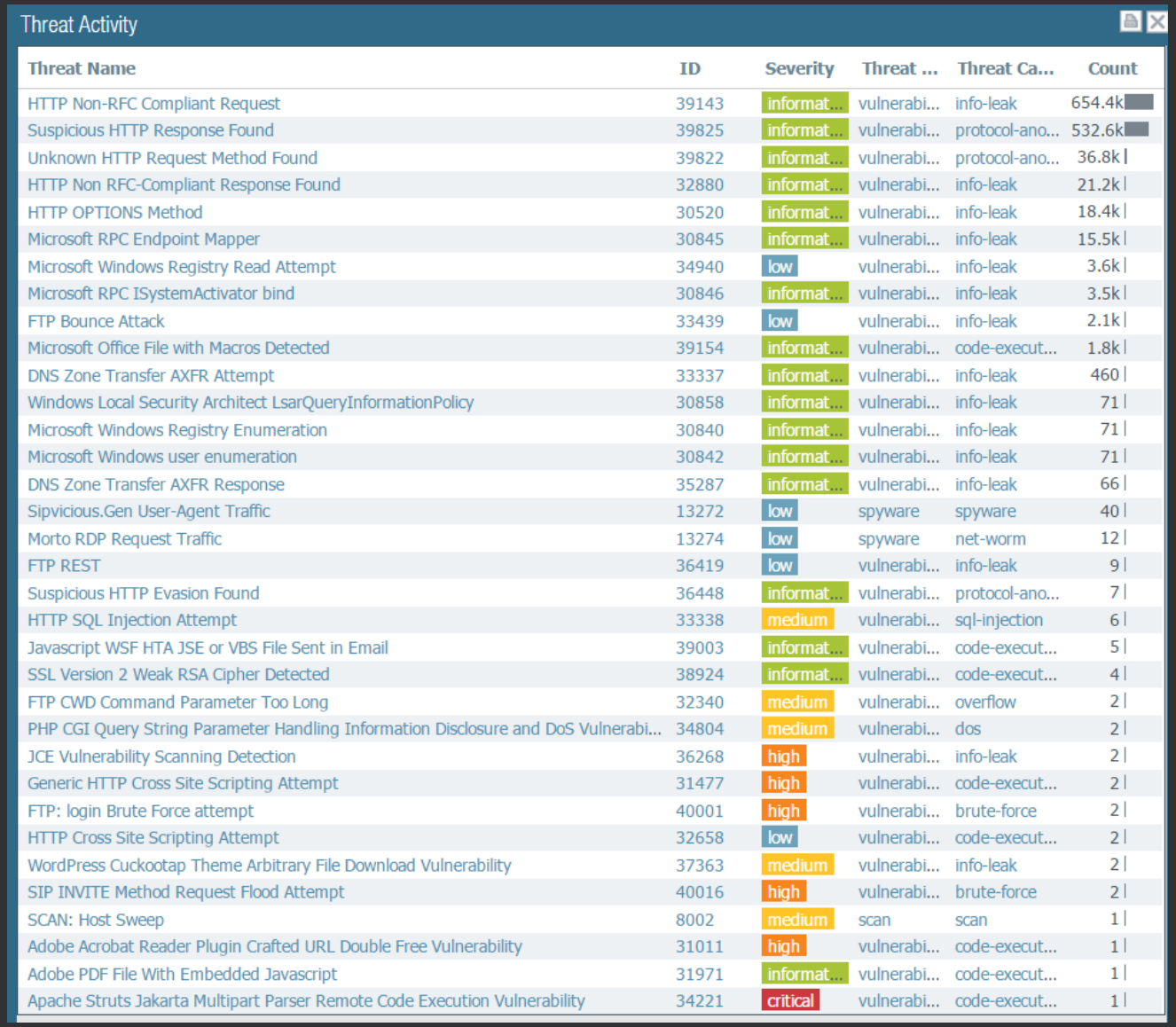
Recursos Técnicos de Segurança da Informação

Recursos Técnicos de Segurança da Informação

- **Equipamentos de Segurança**
  - Garantem a proteção do perímetro das redes do IBGE
- **Controle de Autenticação, Autorização e Auditoria no acesso às redes e sistemas**
- **Sistemas de monitoramento**
  - Gerenciamento das redes, monitoramento da disponibilidade e desempenho dos ativos e circuitos de comunicação
- **Equipamentos e circuitos redundantes**
  - Mantém os serviços e a comunicação disponíveis em caso de falha de um equipamento ou circuito
- **Criptografia, certificados e assinaturas digitais**
  - Garantem o sigilo, autenticidade e integridade da informação
- **Sistemas de proteção**
  - AntiSpam, backup, proteção do EndPoint, análise de vulnerabilidades, desenvolvimento seguro etc.
- **Circuitos de Internet com proteção contra ataques (anti-DDoS)**
- **Sistema Autônomo IBGE**

Recursos Técnicos de Segurança da Informação

- Ameaças identificadas em um único dia!



Threat Activity

Threat Name	ID	Severity	Threat ...	Threat Ca...	Count
HTTP Non-RFC Compliant Request	39143	informat...	vulnerabi...	info-leak	654.4k
Suspicious HTTP Response Found	39825	informat...	vulnerabi...	protocol-ano...	532.6k
Unknown HTTP Request Method Found	39822	informat...	vulnerabi...	protocol-ano...	36.8k
HTTP Non RFC-Compliant Response Found	32880	informat...	vulnerabi...	info-leak	21.2k
HTTP OPTIONS Method	30520	informat...	vulnerabi...	info-leak	18.4k
Microsoft RPC Endpoint Mapper	30845	informat...	vulnerabi...	info-leak	15.5k
Microsoft Windows Registry Read Attempt	34940	low	vulnerabi...	info-leak	3.6k
Microsoft RPC ISystemActivator bind	30846	informat...	vulnerabi...	info-leak	3.5k
FTP Bounce Attack	33439	low	vulnerabi...	info-leak	2.1k
Microsoft Office File with Macros Detected	39154	informat...	vulnerabi...	code-execut...	1.8k
DNS Zone Transfer AXFR Attempt	33337	informat...	vulnerabi...	info-leak	460
Windows Local Security Architect LsarQueryInformationPolicy	30858	informat...	vulnerabi...	info-leak	71
Microsoft Windows Registry Enumeration	30840	informat...	vulnerabi...	info-leak	71
Microsoft Windows user enumeration	30842	informat...	vulnerabi...	info-leak	71
DNS Zone Transfer AXFR Response	35287	informat...	vulnerabi...	info-leak	66
Sipvicious.Gen User-Agent Traffic	13272	low	spyware	spyware	40
Morto RDP Request Traffic	13274	low	spyware	net-worm	12
FTP REST	36419	low	vulnerabi...	info-leak	9
Suspicious HTTP Evasion Found	36448	informat...	vulnerabi...	protocol-ano...	7
HTTP SQL Injection Attempt	33338	medium	vulnerabi...	sql-injection	6
Javascript WSF HTA JSE or VBS File Sent in Email	39003	informat...	vulnerabi...	code-execut...	5
SSL Version 2 Weak RSA Cipher Detected	38924	informat...	vulnerabi...	code-execut...	4
FTP CWD Command Parameter Too Long	32340	medium	vulnerabi...	overflow	2
PHP CGI Query String Parameter Handling Information Disclosure and DoS Vulnerabi...	34804	medium	vulnerabi...	dos	2
JCE Vulnerability Scanning Detection	36268	high	vulnerabi...	info-leak	2
Generic HTTP Cross Site Scripting Attempt	31477	high	vulnerabi...	code-execut...	2
FTP: login Brute Force attempt	40001	high	vulnerabi...	brute-force	2
HTTP Cross Site Scripting Attempt	32658	low	vulnerabi...	code-execut...	2
WordPress Cuckootap Theme Arbitrary File Download Vulnerability	37363	medium	vulnerabi...	info-leak	2
SIP INVITE Method Request Flood Attempt	40016	high	vulnerabi...	brute-force	2
SCAN: Host Sweep	8002	medium	scan	scan	1
Adobe Acrobat Reader Plugin Crafted URL Double Free Vulnerability	31011	high	vulnerabi...	code-execut...	1
Adobe PDF File With Embedded Javascript	31971	informat...	vulnerabi...	code-execut...	1
Apache Struts Jakarta Multipart Parser Remote Code Execution Vulnerability	34221	critical	vulnerabi...	code-execut...	1

OBRIGADO.