Ciber Ataques en el tiempo de crisis y como prevenirlos

Mayo 2020

NOISE
CIBERSEGURIDAD

1. Presentación

- Nelson Chacon, El Salvador
- Maestría en Seguridad de la información y riesgos.
- Certificaciones
  - Auditor ISO 27001
  - Cobit fundamentals
  - Investigador forense digital
  - Seguridad en redes de datos, India.
- Ingeniero en Ciber Seguridad, BlueVoyant, NY, Estados Unidos.
- Fundador de NOISE Ciber Seguridad.
- Líder Capitulo OWASP El Salvador.
- Docente de Maestrías en universidades de El Salvador, Bolivia

Estado actual

- Empresas
  - Nuevos servicios
  - Cambios en configuraciones
  - Falta de monitoreo
  - Transformación Digital.
- Empleados
  - Trabajo desde casa
  - Uso de equipo personal

Riesgos

- Nuevos servicios
  - RDP, VNC, SSH (accesos remotos)
  - VPN (Túneles)
  - Cambio de configuraciones no documentadas
  - Comercio electrónico
  - Video conferencias
  - Monitoreo de servicios críticos
  - Regreso a la normalidad

Riesgos

- Teletrabajo
  - Falta de políticas en equipo local (BYOD)
  - Endpoint protection
  - Monitoreo
  - Exposición de información sensibles
  - Uso de servicios / aplicaciones no oficiales

Riesgos
Teletrabajo-Perdida de control

Ataques

- Phising, mensajes alusivos a la crisis
  - Malware
  - Servicios bancarios
  - Vishing
  - Smishing, SMS
- Spoofing,
  - suplantación de correos empresariales
  - Suplantación de sitios web
  - Estafas

Ataques

- Ransomware
  - Servicios de RDP, SMB
  - Phising
- Aplicaciones Falsas, suplantación las aplicaciones reales.
  - Sitios falsos
  - App móviles falsas

El Salvador RDP

TOTAL RESULTS

380

TOP COUNTRIES

El Salvador

Windows Server 2008 R2 Enterprise

Windows Server 2008 Enterprise

Microsoft Windows Server 2003 Enterprise Edition

Microsoft Windows xp Professional

Windows Server 2012 R2

Windows 7 Professional

NOISE CIBERSEGURIDAD

El Salvador SMB

TOTAL RESULTS

225

TOP COUNTRIES

El Salvador

Shares

Name	Type	Comments
Adjuntos	Disk	
ADMIN$	Disk	Admin remota
B1_SHR	Disk	
C$	Disk	
IPC$	IPC	
SAP	Disk	
SCSW_WORKING_SHARE	Disk	

Shares

Name	Type	Comments
profiles	Disk	Network Profiles Service
users	Disk	All users
groups	Disk	All groups
print$	Disk	Printer Drivers
DOCUMENTOS	Disk	
SCANNER	Disk	
PUBLICA	Disk	
respaldo_pc	Disk	
SCANER_HP	Disk...	

Shares

Name	Ty
ADMIN$	Di
B1_SHR	Di
BSPlanilla	Disk
BSPlanillaT	Disk
C$	Disk
DatosImpresion	Disk
E$	Disk
IPC$	IPC
SAP	Disk

Shares

Name	Type
ADMIN$	Disk
C$	Disk
Citizen_CL-S621	Printer
D$	Disk
Documentos en RED	Disk
Expedientes Empleados	Disk
IPC$	IPC
print$	Disk
Users	Disk

NOISE CIBERSEGURIDAD

Recomendaciones

- Servicios
  - Filtrado por IP/usuario
  - MDM
  - Monitoreo Constante (SOC)
  - Endurecimiento
  - Análisis de vulnerabilidades
  - Test de penetración.
  - Servicios de Resiliencia
  - Matriz de Riesgos Tecnológicos y operacionales
  - Plan de Recuperación de desastres
  - Plan de contingencia
  - Plan de continuidad de negocios

Recomendaciones

- Usuarios
  - Políticas de Seguridad en los Endpoint
  - Uso de VPN
  - Concientización
  - DLP
  - Endpoint EDR

PREGUNTAS

www.noise-sv.com

http://www.facebook.com/noisesv

NOISE
CIBERSEGURIDAD