Seguridad de la información en los años 80 y 90

DOI: 10.29236/sistemas.n175a2

El objetivo de este artículo es presentar como ha cambiado la Seguridad de la información hasta lo que hoy en día se conoce como la Resiliencia Cibernética. En estos últimos años han crecido exponencialmente las herramientas de hackeo y no se necesita un gran conocimiento técnico para hacer ataques y peor aún con el auge reciente de la Inteligencia Artificial y la Computación Cuántica.

Edilberto Sánchez Perdomo

Computación en los años 80s

En los años 80s los **mainframes** eran muy usados en las multinacionales, gobiernos y bancos. IBM era el principal fabricante con sus sistemas **IBM System/370** y luego **System/390**. Otros fabricantes incluían a Univac, **Honeywell** y **Fujitsu**. Usaban lenguajes de programación como **COBOL**, **Assembler**, **PL/1**, **FORTRAN**; Terminales de texto (como el **IBM 3270**) conectadas mediante redes SNA (Systems Network Architecture). **Sistema operativo MVS (Multiple**

Virtual Storage) de IBM. **Sun Microsystems** no fabricó mainframes, pero fue clave en los 80 y 90 con sus **workstations y servidores UNIX**, especialmente bajo su sistema operativo **Solaris**. Fue pionera en la arquitectura **RISC** (SPARC) y en la promoción del **modelo cliente-servidor**, que fue desplazando a los mainframes en muchos entornos.

Burroughs fue uno de los grandes fabricantes de mainframes, especialmente en los años 60, 70 y hasta mediados de los 80. Sus equipos con fuertes sistemas operativos y software de comunicación como BNA jugaron un papel muy importante en Colombia. Sus sistemas eran populares en el sector bancario y gubernamental, conocidos por su fuerte orientación a la seguridad y la transaccionalidad. En 1986, Burroughs se fusionó con **Sperry** para formar **Unisys**, lo que marcó el declive del nombre "Burroughs", aunque sus mainframes Series A con lenguajes poderosos como BPL y de Cuarta Generación como LINC II continuaron evolucionando bajo la marca Unisys. Finalmente, UNISYS le aposto muy tarde al desarrollo de Internet, pero la competencia con la explosión de Windows y de sistemas operativos basados en Unix como Sun Solaris, RISC 6000 y Linux entre otros tomo mucha ventaja. En esta época la mayoría de entidades usaron Internet para mejorar sus sistemas de Front End desde PCs y grandes granjas de servidores de presentación, pero las grandes bases de datos aun residían en los mainframes y servidores centralizados.

Computación en los años 90s

Para los años 90 IBM System/390 evolucionó con mejor capacidad de procesamiento y soporte para tecnologías como TCP/IP, **Introducción del software cliente-servidor**, pero los mainframes siguieron siendo usados para procesamiento de back-end. **Linux y Unix** empezaron a influir en entornos empresariales, aunque los mainframes se adaptaron integrando entornos virtuales. IBM introdujo **VM/ESA**, que permitía múltiples entornos virtuales en un solo mainframe. **Seguridad y fiabilidad**: Se reforzaron, haciéndolos ideales para banca, seguros y gobiernos. **Interfaces gráficas**: Comenzaron a desarrollarse front-ends en PCs conectados a mainframes a través de redes.

Hackers más famosos de estas décadas

Década de los 80s

1. Kevin Mitnick Apodado “El hacker más buscado del mundo” por el FBI. Se infiltró en sistemas de empresas como Nokia, Motorola y Sun Microsystems.

2. Robert Tappan Morris Creador del Morris Worm (1988), uno de los primeros gusanos en Internet. Su ataque colapsó una gran parte de la red ARPANET.

Década de los 90s

1. Adrian Lamo: Conocido como "el hacker nómada", se infiltró en redes como las de Microsoft y The New York Times. Se volvió famoso también por denunciar a Chelsea Manning por filtrar documentos a WikiLeaks.

2. Vladislav Levin Un hacker ruso que robó alrededor de 10 millones de dólares del Citibank usando acceso remoto a sus sistemas.

3. Mafiaboy (Michael Calce) En 2000, con solo 15 años, lanzó un ataque DDoS que tumbó sitios como Yahoo!, CNN,eBay y Amazon.

El robo al Chase Manhattan Bank

En mayo de 1983, Roberto Soto Prieto lideró el desvío de 13,5 millones de dólares de una cuenta del gobierno colombiano en el Chase Manhattan Bank de Nueva York. Suplantando los télex del Banco de la República, el dinero fue transferido primero al Banco Morgan Guaranty y luego a una cuenta cifrada en Suiza. Este robo fue descubierto en octubre de ese mismo año cuando se detectó la ausencia de fondos en una cuenta estatal. Al principio de este caso el Chase no acepto ningún tipo de responsabilidad. El Banco de la Republica contrato a la empresa Británica Control Risk y se comprobó que el Chase acepto unas claves que no eran válidas. Finalmente, el Chase Manhattan tuvo que asumir el valor de este fraude.

El fraude se realizó suplantando un fax que no tenía nada que ver con los sistemas de cómputo centrales del Banco de la República.

Control Risk recomendó al Banco la creación del área de seguridad informática. En este proceso fui seleccionado por tener el mayor conocimiento de la plataforma del Banco como System Programmer y como no se conocía del tema, visite varias entidades importantes a nivel mundial como el Federal Reserve, Bankers Trust, City Bank of New York, Banamex en México y algunos proveedores de tecnología como Burroughs, Cisco, IBM y otros. El área de seguridad informática cubrió rápidamente todos los niveles físicos y lógicos incluyendo mejoras en la seguridad del centro de cómputo en Bogotá y la creación de centros alternos en Medellín, Cali y Barranquilla para contingencia. Para esa época se estudiaron los niveles de seguridad dados por el departamento de defensa de los Estados Unidos TCSEC (Trusted Computer System Evaluation Criteria) que incluían D1, C1, C2, B1, B2, B3 y A y se decidió que el Banco de la República debía por lo menos tener algunas de las características del nivel C2 y B1 y se llevaron a cabo diferentes proyectos a nivel de Pcs, Unix y Sistemas Series A en primera instancia. Así mismo se escogieron

equipos de encripción a nivel hardware para uno de los proyectos más importantes del Banco como lo fue SEBRA (Servicios Electrónicos del Banco de la Republica).

En los años 80 y 90 los sistemas operativos de los mainframes eran muy complejos de entender y configurar; funcionaban en un esquema centralizado y no distribuidos con terminales brutas, lo que los hacía mucho más seguros. Adicionalmente estaban muy protegidos y de hecho se necesitaba de un especialista System Programmer para poder administrarlo. La mayoría de entidades en el mundo carecían de conocimiento en seguridad de la información y solo los sectores de defensa de países avanzados y algunas multinacionales tenían los recursos para proteger sus sistemas.

De hecho, para esta época se crea el NSA (National Security Agency) y contaba con más de 70.000 ingenieros dedicados a seguridad, así mismo entidades como Shell Company desarrollaron estándares de seguridad como el BS7799, que más tarde se convirtió en el estándar ISO27001.

Ciberseguridad y resiliencia cibernética

Ciberseguridad

También se conoce como la seguridad digital o electrónica y es el conjunto de medidas y prácticas que protegen los sistemas informáticos, las redes y los datos de amenazas y ataques cibernéticos, su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información.

El estándar ISO 27001 del año 2013 se enfocó en los sistemas de información tradicionales de los mainframes sin tener muy en cuenta el auge de Internet y todo el tema de Cloud Computing, Computación en Tabletas y la masificación de Teléfonos inteligentes y Redes Sociales. Ya el estándar ISO27001 en su versión del año 2022 trata con más detalle estos temas de Ciberseguridad incorporando ISO27032 a ISO27001:2022. Afortunadamente en Colombia la Superintendencia Financiera forzó el uso del estándar ISO27001 hace más de 20 años y el sector financiero lo tuvo que implementar para cumplir las normativas de la SFC. En años recientes Gartner Group generó SASE (Secure Access Service Edge) el cual ha servido mucho a todo tipo de entidades para tener una postura concreta de Ciberseguridad así mismo lo hizo NIST Cibersecurity Framework (CSF).

Resiliencia cibernética

Hoy en día, La Resiliencia Cibernética se define como la capacidad de una empresa para prevenir, detectar, responder y recuperarse lo más rápido posible de interrupciones en la Infraestructura Tecnológica, incluyendo ciberataques y otros incidentes.

Industrias más vulnerables hoy en día

Las industrias más vulnerables desde el punto de vista de ciberseguridad suelen ser aquellas que manejan grandes volúmenes de datos sensibles, dependen de sistemas digitales críticos o tienen infraestructuras complejas y desactualizadas. Estas son algunas de las más vulnerables:

1. Salud: Alta cantidad de datos personales y médicos. Uso de dispositivos conectados (IoMT) muchas veces mal protegidos. Infraestructura tecnológica antigua en muchos hospitales.

2. Finanzas y banca: Objetivo frecuente por el acceso a fondos y datos financieros. Amenazas comunes: ransomware, phishing, robo de identidad.

3. Energía y servicios públicos: Infraestructura crítica (redes eléctricas, petróleo, agua). Posibles consecuencias físicas y económicas graves.

4. Educación: Menor inversión en ciberseguridad. Redes amplias con múltiples usuarios y dispositivos.

5. Retail y comercio electrónico: Alto volumen de transacciones y datos de tarjetas de crédito. Vulnerables a ataques de POS y robo de identidad.

6. Gobierno: Datos sensibles de ciudadanos y seguridad nacional. A menudo objetivo de ciber espionaje y ataques patrocinados por estados.

7. Industria manufacturera: Uso creciente de IoT con poca protección. Ataques a la cadena de suministro.

Sistemas operativos, bases de datos y ERP más atacados

Según informes recientes de ciberseguridad (como los de IBM, Verizon y CISA)

Sistemas Operativos

1. Windows (especialmente versiones antiguas como Windows 7, Server 2008): Por su amplia base instalada. Vulnerabilidades conocidas (como EternalBlue).

2. Linux (especialmente en servidores): Aunque más seguro por diseño, sigue siendo atacado por malware como ransomware (ej. Linux.Reptile).

3. Android: Muy atacado en dispositivos móviles por su fragmentación y apps maliciosas.

Bases de Datos

1. Microsoft SQL Server: Ataques de inyección SQL y explotación de puertos abiertos.

2. Oracle Database: Ataques a versiones no actualizadas, explotación de CVEs.

3. MySQL/MariaDB: Blanco común por ser muy popular en entornos web.

4. MongoDB: Casos frecuentes de bases expuestas sin autenticación (ataques ransomware de "exfiltración y extorsión").

ERP

1. SAP: Muchas organizaciones no aplican parches de seguridad a tiempo. Ataques a interfaces mal protegidas (como SAP Gateway o SAPRouter).

2. Oracle E-Business Suite: Foco por ser usado en entornos corporativos críticos.

3. Microsoft Dynamics 365: Vulnerabilidades en la nube o por malas configuraciones.

Algunos ciberataques recientes en Colombia

1. **EPM (Empresas Públicas de Medellín):** En 2019, EPM sufrió un ciberataque que afectó varios de sus sistemas informáticos, lo que provocó la interrupción de algunos servicios públicos y la filtración de datos.

2. **Gobierno colombiano**: En diversas ocasiones, entidades gubernamentales han sido blanco de ciberataques. En 2020, hubo informes de que los sistemas del Gobierno fueron atacados, y varios departamentos de la administración pública sufrieron interrupciones. En septiembre de 2023 las entidades gubernamentales que tenían servicios de hosting con IFX Networks sufrieron un ataque masivo de Ransomware.

3. **Keralty**: En noviembre de 2022 la organización multinacional fue víctima de un ataque de ramsomware que afecto los sitios web y operaciones de la empresa y sus subsidiarias como la EPS Sanitas y su servicio de medicina prepagada Colsanitas, las cuales tardaron más de 4 meses en estabilizar sus servicios.

4. **SURA**: La aseguradora SURA sufrió un ataque en 2020, que afectó sus sistemas operativos. Aunque no hubo grandes filtraciones de información, el incidente afectó la disponibilidad de algunos servicios.

Riesgos futuros de ciberseguridad

Los riesgos futuros de ciberseguridad están evolucionando rápidamente con los avances tecnológicos. Algunos de los más relevantes:

1. **Ataques impulsados por inteligencia artificial (IA):** Los ciberdelincuentes están empe-

zando a usar IA para automatizar ataques, mejorar el phishing, y evadir sistemas de defensa. Los deepfakes también se usarán para fraudes, suplantación de identidad o desinformación.

2. **Amenazas a infraestructuras críticas:** Energía, agua, salud y transporte están cada vez más digitalizados. Un ataque exitoso podría causar apagones, colapsos hospitalarios o accidentes masivos.

3. **Internet de las cosas (IoT) vulnerable:** Dispositivos conectados como cámaras, relojes inteligentes o electrodomésticos pueden ser puertas de entrada para los atacantes si no se protegen adecuadamente.

4. **Cibercrimen como servicio:** Plataformas clandestinas ya ofrecen herramientas y servicios para lanzar ataques sin que el comprador tenga conocimientos técnicos, lo que democratiza el cibercrimen.

5. **Amenazas cuánticas:** Las computadoras cuánticas podrían romper los sistemas de cifrado actuales, comprometiendo datos altamente sensibles.

6. **Filtraciones y ransomware más agresivos:** Las extorsiones digitales seguirán creciendo, con grupos más sofisticados y estrategias dobles: cifrado más publicación de los datos robados.

Algunos grupos de Hackers en el mundo

Existen numerosos grupos de hackers en el mundo, algunos con fines delictivos, otros con motivaciones políticas o activistas. Lista con algunos de los más conocidos, clasificados según su motivación principal:

1. **Ciberdelincuentes (motivación: dinero):** FIN7 (o Carbanak Group): Roban tarjetas de crédito y datos bancarios; han atacado a empresas en todo el mundo. Conti / Ryuk / LockBit: Grupos de ransomware que cifran información y exigen rescate, vinculados con redes criminales organizadas.

2. **Hacktivistas (motivación: ideología):** Anonymous: Red global de hackers sin liderazgo central, famosos por ataques DDoS, filtraciones y campañas contra gobiernos y corporaciones. Killnet: Grupo pro-ruso que ha atacado infraestructuras digitales de países que apoyan a Ucrania. Guacamaya: Hackers latinoamericanos que han filtrado documentos militares de gobiernos en la región (México, Chile, Colombia).

3. **APTs (Amenazas persistentes avanzadas, motivación: espionaje):** APT28 (Fancy Bear):

Vinculado al gobierno ruso (GRU), involucrado en hackeos políticos como el del Comité Demócrata en EE.UU. en 2016. APT29 (Cozy Bear): También asociado a Rusia, experto en ciberespionaje. Lazarus Group: Vinculado a Corea del Norte; responsable del ataque a Sony Pictures y el ransomware WannaCry. Charming Kitten: Asociado a Irán, enfocado en espionaje político y académico. APT41: Vinculado a China; mezcla espionaje estatal con robo financiero.

Herramientas de Hacking ético (O no ético)

Existen muchas herramientas de hacking ético (o no ético) utilizadas para evaluar o comprometer la seguridad de sistemas informáticos.

1. **Recolección de información (OSINT):** Maltego: Visualiza redes y relaciones entre personas, organizaciones o IPs. Recon-ng: Framework en Python para recopilar datos de objetivos desde fuentes públicas. TheHarvester: Extrae correos, dominios, hosts desde buscadores y bases de datos públicas.

2. **Escaneo de vulnerabilidades:** Nmap: Escaneo de puertos, detección de sistemas operativos y servicios activos. Nessus: Escáner de vulnerabilidades profesional, usado por empresas y pentesters. OpenVAS: Escáner de código abierto para detectar fallos de seguridad.

3. **Explotación de vulnerabilidades:** Metasploit Framework: Herramienta poderosa para desarrollar y ejecutar exploits. BeEF (Browser Exploitation Framework): Explotación de vulnerabilidades en navegadores web. SQLmap: Automatiza ataques de inyección SQL para extraer bases de datos.

4. **Ataques de red:** Wireshark: Analizador de tráfico en tiempo real, útil para detectar paquetes sospechosos. Aircrack-ng: Cracking de redes Wi-Fi (WEP/-WPA/WPA2) mediante sniffing y fuerza bruta. Ettercap: Ataques MITM (man-in-the-middle) y sniffing de tráfico en redes LAN.

5. **Ingeniería social y phishing:** Social-Engineer Toolkit (SET): Automatiza la creación de ataques de phishing, clonado de páginas y correos maliciosos. Gophish: Plataforma para simular campañas de phishing de manera ética (usada en pruebas corporativas).

6. **Fuerza bruta y cracking:** Hydra: Herramienta para ataques de fuerza bruta sobre múltiples protocolos (SSH, FTP, HTTP, etc.). John the Ripper: Cracking de contraseñas (archivos hash). Hashcat: Crackeo avanzado de hashes, compatible con GPUs.

Principales tipos de ciberataques con IA

1. **Phishing y Spear Phishing Automatizado:** IA genera correos, chats o mensajes altamente personalizados usando información pública (redes sociales, correos filtrados). Aumenta la tasa de éxito del engaño.

2. **Deepfakes:** Videos o audios falsificados con IA para suplantar identidades (ej. directores financieros o políticos). Se han usado para fraudes bancarios, manipulación mediática y extorsión.

3. **Malware que aprende y se adapta:** IA puede analizar entornos de red y adaptarse para evitar detección. Malware polimórfico: cambia su código o comportamiento usando aprendizaje automático para esquivar antivirus.

4. **Ataques a modelos de IA:** Envenenamiento de datos (data poisoning): insertar datos corruptos durante el entrenamiento de un modelo. Evasión (adversarial attacks): inputs maliciosos diseñados para engañar modelos (ej. visión computarizada, reconocimiento facial).

5. **Automatización de ataques:** Bots inteligentes que escanean redes, encuentran vulnerabilidades y lanzan ataques sin intervención humana. Reducción del tiempo de ataque de días a minutos.

6. **Ataques a sistemas de ciberdefensa basados en IA:** Los atacantes pueden estudiar el comportamiento de sistemas de defensa inteligente para evadir detecciones, “engañarlos” o desactivarlos.

Computación cuántica

La computación cuántica representa una revolución tecnológica con un gran potencial tanto para mejorar como para amenazar la ciberseguridad. Aunque su uso en ataques reales aún es limitado, los expertos coinciden en que su impacto será profundo en los próximos 5 a 10 años.

Posibles usos en ciberataques futuros

1. **Rompimiento de criptografía tradicional:** Los algoritmos de cifrado más comunes hoy (como RSA, ECC) podrían ser rotos en segundos con una computadora cuántica suficientemente potente.

2. **Amenazas a blockchain:** Las criptomonedas y contratos inteligentes que usan algoritmos como SHA-256 o ECDSA pueden volverse vulnerables.

3. **Ataques a firmas digitales y autenticaciones:** Cualquier sistema que use firmas digitales

(correo, software, certificados) corre riesgo de ser falsificado.

4. **Espionaje retroactivo:** Los atacantes podrían estar almacenando comunicaciones cifradas actuales para descifrarlas en el futuro cuando tengan acceso a computadoras cuánticas ("store now, decrypt later").

Recomendaciones básicas

Tener alineados los tres ejes de una empresa (Gente, Procesos y Tecnología) desde el punto de vista de Resiliencia Cibernética

1. **Gente**: Capacitación, sensibilización, entrenamiento y certificaciones
2. **Procesos**: Políticas, Normas, Procedimientos y estándares. Plan Continuidad del Negocio incluyendo DRP, Auditorías y Oficial de seguridad de la información.
3. **Tecnología**: Arquitectura de seguridad basada en SASE de Gartner Group y NIST incluyendo firewalls, End Point Security con antivirus antimalware y DLP para fuga de información, VPNs, Autenticación multifactor, Sistemas de evaluación de compromiso continuo y SOC (Security Operation Center).

***Edilberto Sánchez Perdomo**, (gerencia.lutsagroup@gmail.com). Ingeniero de Sistemas y Computación Universidad de los Andes (1981). CEO lutsa group: Miembro juntas directivas en temas de Ciberseguridad. SGSI basado en ISO27001:2022 para Servimercadeo. Banco de occidente Gerente Auditoría Tecnología. UNISYS Gerente Seguridad Informática LATAM preventa SOC (Reston Virginia); Arquitectura Seguridad Informática ISA; Petrobras (Brasil) cumplimiento ISO 27001; secretaria Seguridad Publica (México) Análisis de Impacto al Negocio; Banesco (Venezuela) Plan Continuidad Negocio. PwC Gerente Technology Risk Services Grupo Aval Modelo seguridad informática para Portal Avalnet, ISA, Conavi, Bancolombia, EPM y Banco de la República system programmer, Creador y director Unidad de Seguridad Informática (1986).*