MILESTONES
OF INFORMATION SECURITY

La Seguridad de la Información, hoy más conocida como Ciberseguridad, ha sido necesaria desde la existencia de las mismas redes de computador. Los antecedentes más remotos dan cuenta de como el ofrado de información que se transmitia por medios como la radio o el telegrafo fueron los primeros sistemas de protección utilizados en el siglo pasado. También es de notar que parte del resultado de la Segunda Guerra Mundial fue dado a que Alan Turing y su equipo fueron capaces de descifrar el Código de los Alemanes y por ende el conocimiento de los planes con anticipación.

Esta es una crónica breve sobre 20 de los principales hitos y/o algunos incidentes de seguridad de la información en los tiempos modernos, y posteriores, a la aparición de internet.

1988 — **I-WORM**

Creado por Robert Morris, código que se replicaba a si mismo y significó la afectación del funcionamiento de cerca del 10% de los equipos conectados a Internet.

1994

USD 10 millones del Citibank, es la cifra que robaron hackers rusos a través del acceso a un sistema de Dial-Up del Banco (Financial Institutions Citibank Cash Manager).

SPAM comercial

Caso "Green Card Spam", aparece cuando usuarios del servicio Usenet propagan avisos de servicios legales de inmigración.

1996

Creado el Common. Criteria, por parte de los Gobiernos de Alemania, Canadá, Estados Unidos, Francia, Holanda y el Reino Unido, con el fin de contar con un sistema unificado de evaluación de productos de seguridad.

Nace Digiware.

1998

Se lanza el CVE, o diccionario de vulnerabilidades que sintetiza las vulnerabilidades o exposiciones identificadas de seguridad y estrategias de mitigación, bajo una codificación unificada.

1999

Se "rompe" el código DES de 56-bits en menos de 24 horas. RSA da un premio de USD $10.000 por esto.

IIIII = 5 años de prisión

recibió Kevin Mitnick, el hacker más famoso del mundo hasta ese momento.

2000

Un ataque distribuido de DDoS, "baja" temporalmente múltiples sitios populares de Internet, tales como CNN, Yahoo, eBay, Dell y Amazon.

= 45 millones de computadores

afectados por el virus "I love You", via correo electrónico.

2003

El grupo Anonymous es creado y se vuelve famoso por ejecutar ataques coordinados contra "blancos" específicos. Se identifican por una máscara de Guy Fawkes.

2004

MY-DOOM

Worm de internet que se propaga afectando 1 de cada 12 correos.

2007

Estonia es víctima del primer ataque estructurado contra la infraestructura informática y de telecomunicaciones, de un país afectando el gobierno, los medios de comunicación y las redes de celular a través de ataques de DDoS y botnets sofisticados.

Otro ataque DDoS contra los 13 servidores primarios de DNS en el Mundo, deshabilitando efectivamente a 5, siendo considerado el primer ataque para afectar el funcionamiento total de internet.

2010

Se descubre la operación Aurora: ataques dirigidos desde China contra compañías de tecnología de E.E.U.U., como Adobe, Juniper, Yahoo, Symantec, entre otras, con el fin de tener acceso a sus secretos industriales.

EEUU

2011

RSA Security anuncia que ha sido víctima de un ataque sofisticado que permitió acceso a los sistemas que manejan el desarrollo de código de autenticación de dos factores de esta firma.

2013

Edward Snowden filtra información confidencial, que obtiene a través de acceso a bases de datos del NSA y que publica con apoyo de Wikileaks, mostrando los alcances de una filtración de información confidencial.

Target es victima de un ataque sobre sus Point-Of-Sales, donde son capturados millones de tarjetas, débito y crédito debido a un malware. Reconocido como una de las fugas de tarjetas de crédito más grandes de la historia.

2014

Un grupo de hackers autodenominado como Guardians of Peace, filtra información confidencial de Sony, incluyendo emails de los principales ejecutivos e información propietaria sobre películas, estrategias y salarios de los empleados, entre otra información.

2015

En un artículo de la revista Wired aparecé publicado el primer caso de hacking sobre un vehiculo en movimiento, extendiendo las preocupaciones del mundo de Internet a la realidad física interconectada.

STUXNET INFECTED

Stuxnet, un gusano malicioso de bastante sofisticación, que se cree que fue desarrollado por una o varias naciones, afectó el desarrollo de programa de desarrollo nuclear de Irán al afectar los sistemas PLC de una fábrica de enriquecimiento de Uranio.

DIGIWARE
Su aliado en seguridad de la información

Éstos son apenas algunos de los casos que han salido a la luz pública. Diariamente son publicados nuevos casos y estos sucesos ya son parte de la vida diaria. Queda el interrogante de lo que vendrá ante la continua, y con mayor profundidad, automatización de nuestra vida diaria.