Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

Seminario

“Presente y Futuro de la Auditoría Interna de Gobierno: Hacia la Institucionalidad del CAIGG”

Santiago, 17 de octubre de 2018

Ciberseguridad

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia

Ciberseguridad

Carlos Silva

Certified Information Systems Auditor (CISA), Licenciado en Informática, Master en Gestión de Proyectos

Consultor Internacional

Sobre el conferencista

Carlos Silva

Certified Information Systems Auditor (CISA)

Consultor Internacional

<

- 2018 a la fecha Gerente de Infotecnología, Dirección Adjunta de Rentas Aduaneras
- 2016 -2017 Cowater-Sogema Internacional Inc. Latin America Audit ExpertOttawa, Canadá, Consultor Experto para Latinoamérica de Auditoría de Sistemas de Información y Comunicaciones, Implementación de Gobierno y Gestión de las Tecnologías de la información (TI), Análisis y Evaluación de Riesgos y elaboración de Planes de Contingencia.
- 2017, Banco Nacional de Desarrollo Agrícola, Gerente de Tecnología, • Implementación de mejoras en el Core Bancario BYTE e implementación de nuevos servicios financieros
- • Implementación de gobierno y gestión de TI empresarial, • Análisis y evaluación de riesgos y elaboración de Planes de Contingencia, • Soporte para la creación de políticas institucionales de TI, asesoramiento para la creación de comités tecnológicos de información, evaluación de procesos y controles de TI, elaboración de procesos de planificación de TI, implementación de medidas de seguridad informática, • Supervisión y monitoreo de la plataforma tecnológica del banco
- 2016-2017 Contraloría General de la República de Cuba, La Habana, Cuba, • Facilitador COBIT5, • Implementación del marco comercial para la gobernanza y la gestión de las TI empresariales
- - 2005 – 2017, TRIBUNAL SUPERIOR DE CUENTAS; Director de Tecnología, Experiencia en realización de auditorías informáticas integrales y evaluación de estructuras de gobierno de Tecnologías de la Información (TI) en varias entidades gubernamentales del Gobierno de Honduras

Ciberseguridad

Contexto Actual

El grado de dependencia de la sociedad respecto de las tecnologías de la información y el ciberespacio crece día a día. Nos encontramos con la implantación creciente del Internet móvil y la consiguiente proliferación de dispositivos móviles (acceso mediante todo tipo de dispositivos, teléfonos inteligentes, tabletas, automóviles, trenes, aviones, autobuses, barcos, …), de las tecnologías cloud computing, la virtualización, o el avance imparable de las redes sociales y de los restantes medios sociales. Todo esto unido a la difusión también cada día mayor de las nuevas tecnologías en torno a la geolocalización, realidad aumentada, la web en tiempo real o el Internet de las cosas (acceso a la red mediante todo tipo de «cosas», sensores, electrodomésticos, herramientas tecnológicas, etc.

Las infraestructuras críticas de los países, están soportados con tecnología, con el fin de prestar mejores servicios y brindar protección a sus ciudadanos; por otro lado, las empresas luchan por ganar valor apoyándose en la tecnología.

La tecnología nos brinda muchos beneficios, pero trae consigo una gran cantidad de riesgos, que es necesario conocerlos y gestionarlos.

La multiplicidad de potenciales atacantes han incrementado los riesgos y amenazas que pueden poner en graves dificultades los servicios prestados por las administraciones públicas, las infraestructuras críticas o las actividades de las empresas y ciudadanos.

Información

- Es uno de los activo más valioso de una organización y se debe proteger adecuadamente, independientemente de como se maneje, procese, transporte, almacene o deseche.

- El activo central a proteger del cibercrimen y de la ciberguerra es la información de la empresa en sí, incluyendo información de identificación personal y demás activos privilegiados.

Ciberseguridad

- La ciberseguridad se refiere a todas las medidas de protección empresariales e individuales frente a ataques intencionados, violaciones de seguridad e incidentes, así como de sus consecuencias.

- La ciberseguridad se encarga principalmente de aquellos tipos de ataque, violaciones de seguridad o incidentes dirigidos, sofisticados y difíciles de detectar o gestionar.

- La ciberseguridad debería estar alineada con el resto de aspectos de la seguridad de la información en la empresa, como ser la gobernanza, la gestión y la auditoria de TI.

Ciberseguridad

La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales. Estos ataques generalmente están dirigidos a acceder, cambiar o destruir información sensible; extorsionando dinero de los usuarios; o interrumpir los procesos comerciales normales.

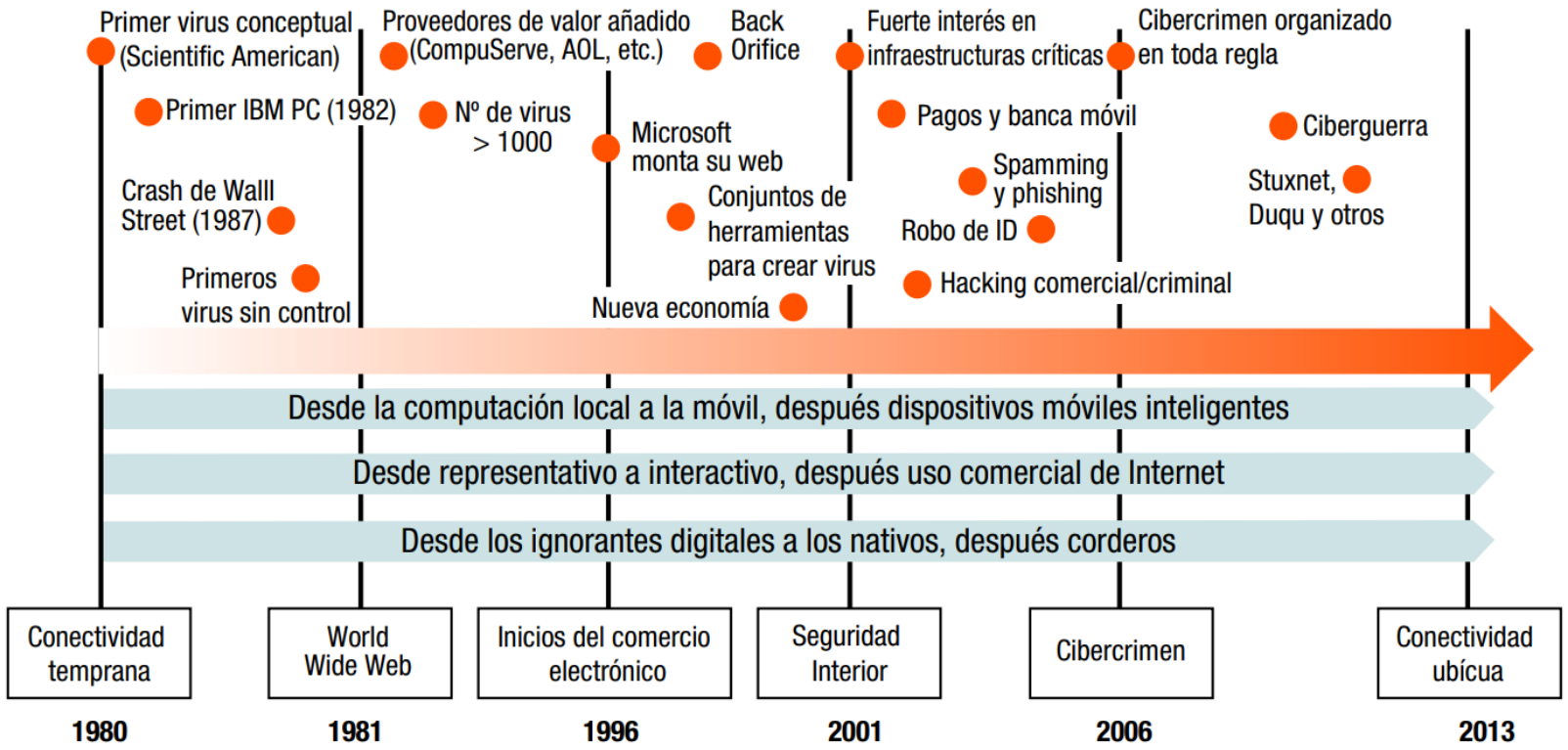
Implementar medidas efectivas de seguridad cibernética es particularmente difícil hoy en día porque hay más dispositivos que personas y los atacantes se están volviendo más innovadores.

Ciberseguridad

Las palabras ciberseguridad, cibercrimen y ciberguerra han tomado relevancia en el mundo de la seguridad en general.

Esto es debido, en parte, a la evolución tecnológica y, en mayor medida, al incremento en las violaciones de seguridad, actos criminales y a la presencia de armas de guerra basadas en la información.

Línea del Tiempo del Ciberespacio



Fuente: von Roessing, Rolf M., 2012

cada fase con sus propias características y consecuencias:

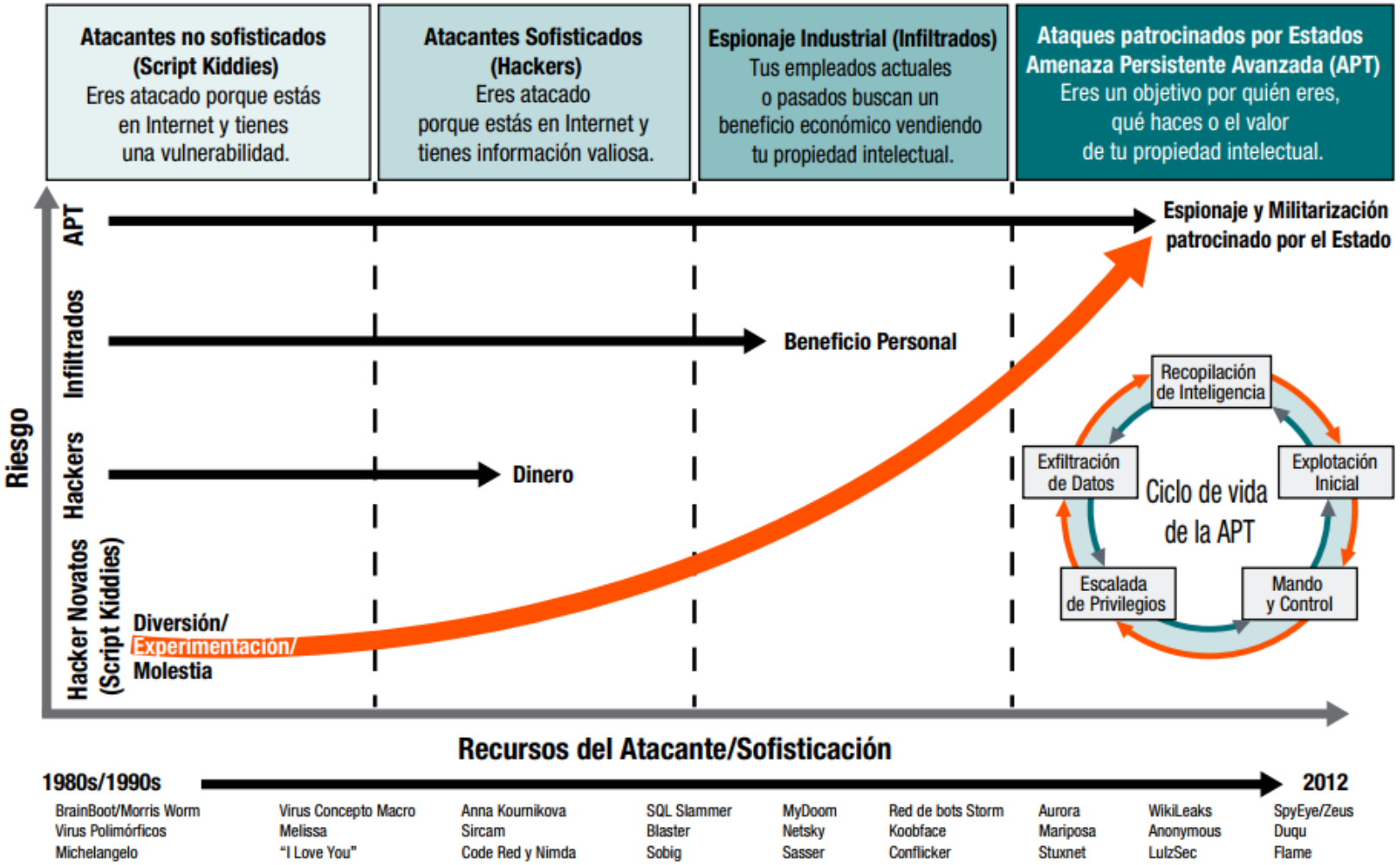
Línea del Tiempo del Ciberespacio

- Desde 2010, el número de amenazas, escenarios de riesgo y vulnerabilidades han crecido casi exponencialmente.

- La ciberseguridad se ha desarrollado como un nuevo campo de interés, ganando atención política y social.

- Los gobiernos y las empresas del sector público están involucrándose en ciberdefensa así como, en algunos casos, capacidad ofensiva y de ataque.

Evolución de las Amenazas



Fuente: ISACA, *Responding to Targeted Cyberattacks*, EE.UU., 2013, figura 2

Cibercrimen y Amenazas Persistentes Avanzadas (APTs)

Las APTs incluyen ataques, violaciones de seguridad, infiltraciones y otros eventos relevantes para la seguridad con un nivel de esfuerzo (o sofisticación) alto o muy alto y un enfoque dirigido a empresas y/o individuos específicos. En la mayoría de los casos, esto comprende una cantidad considerable de investigación de fondo y recopilación de inteligencia, así como una planificación y preparación detallada.

Normalmente, una APT se realiza como una serie de pasos diseñados para maximizar el impacto en el objetivo:

- Reconocimiento/investigación del objetivo
- Planificación
- Explotación/infiltración/entrada
- Comando y control
- Escalada de privilegios, derechos de acceso y aumento paulatino del control del objetivo
- Movimiento lateral e inclusión de objetivos de oportunidad
- Consecución del objetivo inicial, establecimiento de persistencia
- Borrado de rastros

Muchas APTs tienen su origen en el entorno del crimen profesional, crimen organizado y terrorismo.

Ciber-vulnerabilidades, Amenazas y Riesgos

Vulnerabilidad	Amenaza	Riesgo e Impacto
Phishing dirigido	Los atacantes pueden ganar acceso a través de un payload de phishing o combinado con medidas de seguimiento socio-técnicas.	Pérdida o filtración inicial de datos conduciendo a impactos secundarios financieros y operacionales
Abrevadero (*Water holing*)	Los atacantes pueden obtener control de sitios web atractivos con el consecuente control de los visitantes.	Errores de comportamiento iniciales que conducen a un impacto operacional y financiero
APT inalámbrico/ móvil	Los ataques pueden comprometer los canales inalámbricos y/o dispositivos móviles para habilitar un control temporal o permanente.	Control parcial o total de una o más instalaciones inalámbricas y/o dispositivos móviles; impacto directo o indirecto sobre todas las aplicaciones y servicios críticos de TI
Día-Cero	Ataques que usan exploits de día-cero para evitar las defensas existentes.	Control parcial o total de aplicaciones y sistemas/infraestructura subyacente, llegando a ocasionar un impacto en las operaciones

Ciber-vulnerabilidades, Amenazas y Riesgos

Privilegios excesivos	Pueden ocurrir ataques internos mediante el uso de privilegios y derechos de acceso inapropiados.	Control total y (técnicamente) legítimo fuera de los límites del GRC de la organización, impactos secundarios financieros, de operaciones y de reputación
Ingeniería social	Los atacantes se aprovechan de vulnerabilidades sociales para conseguir acceso a información y/o sistemas.	Control total o parcial de objetivos humanos, con el consecuente compromiso en el lado de TI, impactos secundarios en el bienestar personal/individual
APT en el entorno doméstico	Ataques que se aprovechan del hecho que los entornos domésticos pueden estar menos protegidos que los entornos corporativos.	Control parcial o total de aplicaciones, sistemas e infraestructuras domésticas, impactos secundarios financieros, de operaciones o de reputación, incluyendo impactos en el bienestar personal/individual
APT extendido a la infraestructura de TI	Los ataques pueden tener como objetivo la infraestructura TI subyacente en los procesos críticos de la organización.	Total control de la infraestructura, control de riesgo extendido, incluyendo infraestructuras públicas o socios de negocio
APT en infraestructura técnica ajena a TI	Los ataques pueden saltar la barrera entre TI y otras infraestructuras críticas de la empresa.	Control total o parcial de la infraestructura técnica y ajena al estándar de TI, p. ej. control de supervisión y adquisición de datos (SCADA), impacto en operaciones secundarias
Explotación de socios de negocio/ proveedores	Ataques a socios o proveedores de confianza, comprometiendo software o entregables claves.	Ataque inicial a través del TI corporativo dirigido a terceras partes, con un impacto financiero, de operaciones y de reputación

Software malintencionado (malware)

Los ataques APT utilizan software malintencionado, comúnmente conocido como malware, para aprovechar su alcance y capacidad.

El malware puede ser diseñado para ayudar a acceder a sistemas informáticos específicos, robar información o interrumpir las operaciones de los servicios.

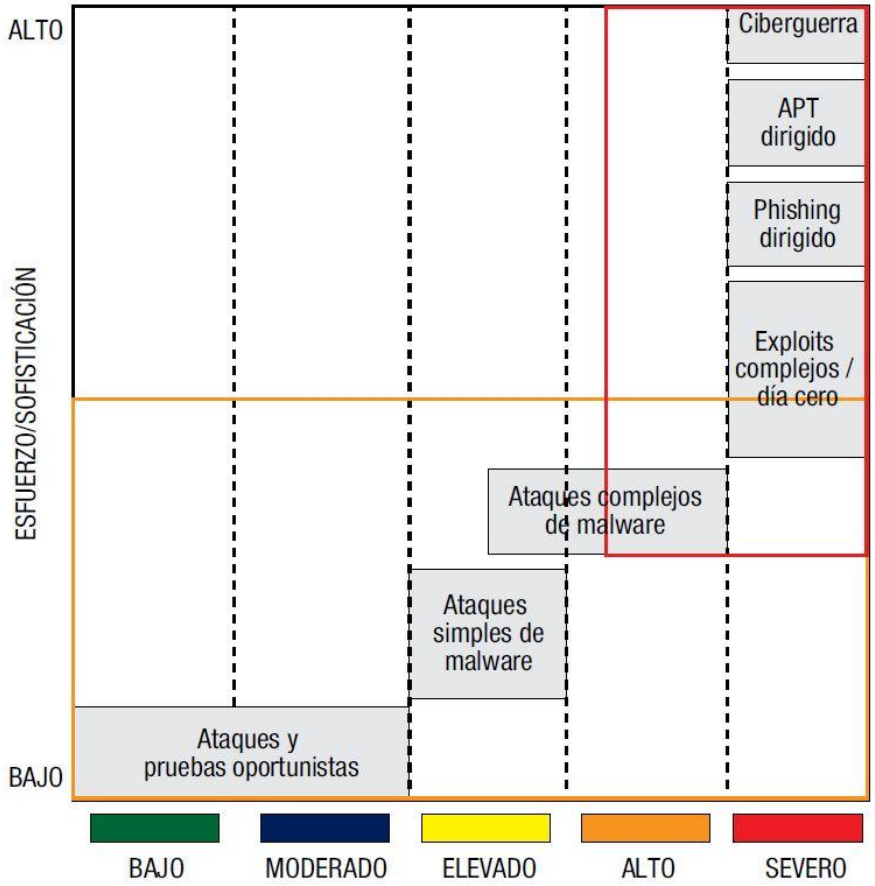
Existen varios tipos de malware, siendo las categorías más importantes los virus informáticos, los gusanos de red y los caballos de Troya, que se distinguen por la forma en que funcionan o se propagan. También se utilizan otros términos para describir tipos más específicos de malware, caracterizados por su propósito.

Ejemplos: Software malintencionado (malware)

- El spyware es una clase de malware que reúne información sobre una persona u organización sin el conocimiento de la persona o la organización.
- El adware es una clase de malware diseñado para presentar anuncios (generalmente no deseados) a los usuarios.
- Ransomware es una clase de malware extorsionador que bloquea o codifica los datos o funciones y exige un pago para desbloquearlos.
- Keylogger es una clase de malware que secretamente graba las pulsaciones del teclado del usuario y, en algunos casos, el contenido de la pantalla.
- Rootkit es una clase de malware que oculta la existencia de otro tipo de malware mediante la modificación del sistema operativo subyacente.

Distribución del Esfuerzo y la Severidad de Varios Ataques

Representa cómo el impacto potencial (desde bajo a severo) se corresponde con un incremento del esfuerzo técnico necesario para preparar y desplegar ataques.



Una breve historia corta de los ataques

Flame fue descubierto por el equipo nacional de respuesta a emergencias informáticas de Irán en 2012. Se utilizó para organizar ataques sofisticados de ciberespionaje en ministerios gubernamentales, instituciones educativas e individuos en países del Medio Oriente, infectando a alrededor de 1,000 máquinas en Irán, Israel, Sudán, Siria, Líbano, Arabia Saudita y Egipto.

Una breve historia corta de los ataques

El gusano Stuxnet, descubierto en junio de 2010, fue la primera pieza de malware encontrada en el dominio público que está diseñado para espiar y subvertir los sistemas de proceso industrial.

Este gusano fue desarrollado para atacar las instalaciones nucleares de Irán.

Se informó que el malware había causado daños considerables a las centrifugadoras en el laboratorio de enriquecimiento nuclear de Natanz en Irán.

Una breve historia corta de los ataques

Octubre Rojo, un programa de malware diseñado para robar secretos de gobierno y organizaciones de investigación (incluyendo datos de dispositivos móviles), fue descubierto en octubre de 2012 por la firma rusa Kaspersky Lab.

Se cree que han estado operando en todo el mundo durante al menos cinco años antes de su descubrimiento, robando una amplia variedad de información, incluyendo secretos diplomáticos, organizaciones de comercio, militares, aeroespaciales, de energía e investigación en Rusia, Irán, Estados Unidos y al menos otros 36 países.

Ciberguerra

Cuando los estados o agencias nacionales participan en ataques a infraestructuras críticas o a organizaciones, las amenazas aumentan por el hecho de que los atacantes pueden tener —por definición— recursos ilimitados a su disposición. Esto incluye el tiempo, dado que las operaciones militares o gubernamentales pueden dedicar varios años desde la idea inicial hasta el despliegue.

Impacto del Cibercrimen y la Ciberguerra en los Negocios y la Sociedad

El cibercrimen y la ciberguerra, como amenazas emergentes, han llevado a una variedad de impactos sobre los individuos, empresas y sociedades. La aparición gradual de la delincuencia organizada y la guerra de información avalada por los gobiernos han ocasionado, primero, un impacto en objetivos expuestos tales como empresas con una atractiva cartera de propiedad intelectual o de otros valiosos activos de información.

El conjunto inicial de los impactos se materializó a menudo como:

- Robo de datos competitivos / inteligencia competitiva, incluyendo espionaje económico

- Robo de propiedad intelectual o de secretos comerciales, apropiación indebida de activos

- Fraude financiero, tarjetas de crédito y otros más amplios robos de identidad, suplantaciones y transacciones fraudulentas

Impacto del Cibercrimen y la Ciberguerra en los Negocios y la Sociedad

Es interesante hacer notar que el cibercrimen, en su forma actual, ha tomado rápidamente un impulso que no había sido previsto ni por los observadores más pesimistas. Ha aumentado de un mero 1% del total de delitos económicos (en 2009) a un significativo 30% a la fecha, superando por varios órdenes de magnitud a muchas otras formas de delitos como el lavado de dinero o el espionaje.

Por el contrario, la ciberguerra ha seguido siendo algo especulativo en términos de números, pero se situó firmemente en la agenda internacional cuando los ejemplares de malware Stuxnet y Duqu se desplegaron en el medio.

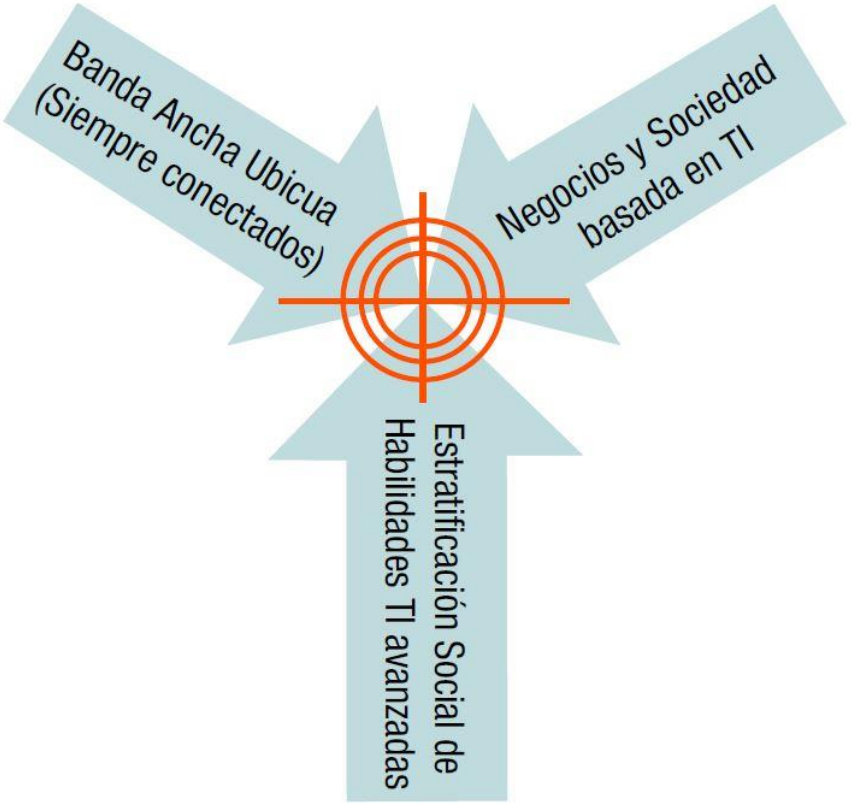
Impacto del Cibercrimen y la Ciberguerra en los Negocios y la Sociedad

Efectos posteriores del cibercrimen, ciberguerra y otras amenazas relevantes se han extendido a través de las empresas y en redes sociales, y ahora se están dirigiendo a casi cualquier capa de usuario y contexto. Los impactos se han multiplicado e incluyen:

- Activismo/hacktivismo y grupos poco organizados.
- Chantaje, extorsión y estafas.
- Recopilación de datos y rastreadores de redes sociales.
- Cambios de apariencia, exposición, difamación.
- Redes de bots y otros fenómenos de malware masivo.
- Denegación de servicio.
- Terrorismo

Tendencias y Elementos de Cambio

Las tres grandes tendencias —o elementos de cambio—han creado, tanto el motivo como la oportunidad, para diversas formas de violaciones de ciberseguridad y actividades delictivas.



Impacto del Cibercrimen y la Ciberguerra en los Negocios y la Sociedad

En el futuro, es probable que las siguientes explicaciones de las principales tendencias y elementos de cambio causen un aumento, incluso mayor, en el cibercrimen y otras amenazas graves, a menos que se pueden idear estrategias de ciberseguridad capaces de ofrecer defensas convincentes a organizaciones e individuos.

Impacto de Negocio y Organizacional

Los incidentes y ataques imputables al cibercrimen son cada vez más caros y dañinos para las empresas.

- Interrupción de procesos críticos de negocio
- Invocación de los planes de gestión de crisis y continuidad de negocio
- Extensa verificación de integridad y confidencialidad de los datos/información,
- Trabajo adicional de investigación interna organizacional/disciplinaria
- Degradación del rendimiento del negocio debido a la cooperación con agencias de la ley externas
- Costes de investigación forense
- Daños reputacionales
- Pérdida de confianza
- Pérdida de cuota de mercado y ventaja competitiva
- Ataques relacionados o incidentes debidos al activismo consiguiente o a seguidores oportunistas

Impacto Individual y Social

- Para los individuos, en el contexto general de la sociedad, el cibercrimen y la ciberguerra han introducido un gran conjunto de nuevos riesgos y amenazas que, a menudo, no son entendidos o lo son de manera insuficiente. De forma simultánea, los individuos están —por regla general— menos protegidos contra cualquier forma de ataque

- Dado que uno de los elementos de cambio decisivos en cuanto a seguridad es la segregación y estratificación de habilidades TI profundas, la posibilidad del individuo para defenderse contra el cibercrimen y la ciberguerra disminuirá en vez de crecer, al menos que a corto plazo se consiga un cambio en la formación.

- El personal de las empresas está sujeto a reglas de gobierno, gestión de riesgos y auditoría. Como resultado, las empresas son (cuando menos) un entorno protegido en el que la gente experimenta menor riesgo de ser atacado que en el plano individual.

Impacto Legal y Regulatorio

- La presencia del cibercrimen y la ciberguerra ha dado lugar a un gran número de iniciativas legislativas y regulatorias a escala mundial. La ciberseguridad está gobernada por un número importante de actas y regulaciones, con estipulaciones cada vez más detalladas para el sector público y las empresas.

- En la práctica, el panorama internacional de leyes y regulaciones de ciberseguridad es bastante diverso. Dependiendo de los diferentes aspectos de la seguridad,se presupone que algunos países proporcionan puerto seguro al cibercrimen, mientras que otros han sido acusados de participar activamente en la ciberguerra.

- El impacto total, en un sentido legal y regulatorio, está todavía por verse. Sin embargo, una proporción significativa de leyes y regulaciones aprobadas hasta la fecha han demostrado su utilidad para el fortalecimiento de la ciberseguridad.

- En aquellas partes en que se han establecido normativas que establecen los fundamentos de una seguridad razonable, tanto el sector público como las empresas han obtenido beneficios considerables.

Infraestructuras críticas

Es el conjunto de activos tecnológicos indispensables, que interactúan entre sí para brindar servicios vitales a los habitantes de un país.

Los activos pueden ser instalaciones físicas o virtuales, redes de datos, redes industriales, sistemas de información, bases de datos, sistemas de control industrial, procesos automatizados o cualquier otro componente tecnológico que permite la prestación o el monitoreo de un servicio esencial para el bienestar de la población y el sostenimiento de la economía de un país.

La falta de controles de ciberseguridad para proteger estos activos origina un grave riesgo para una nación.

Infraestructuras críticas

Algunos de los servicios vitales que generalmente tienen activos con infraestructuras críticas son:

- Telecomunicaciones
- Energía
- Servicios financieros
- Transporte
- Comercio
- Agua
- Salud
- Seguridad
- Industria (alimentación, petróleo, etc.)

Desafíos

- Implementar legislación adecuada tanto en el fondo (tipos penales) como en la forma (normas de investigación y prueba)
- Contar con acuerdos internacionales de cooperación
- Adoptar Estándares Internacionales
- Implementar Políticas Nacionales de Ciberseguridad
- Centros de Respuesta frente a Incidencias de Seguridad Informática (CSIRT)
- Otros

Chile y EE.UU. sellan acuerdo en ciberseguridad: desde tecnologías informáticas hasta cooperación militar

Fuente: https://www.fayerwayer.com/2018/09/chile-ee-uu-acuerdo-ciberseguridad/

Chile y EE.UU. sellan acuerdo en ciberseguridad: desde tecnologías informáticas hasta cooperación militar

Ambos países se comprometen a trabajar juntos en promover y desarrollar el creciente consenso internacional en el marco de un comportamiento responsable del estado en el ciberespacio, e impulsar esfuerzos en las Américas para construir alianzas confiables entre los países de ideas afines. Ambos países además afirman la importancia de la cooperación entre estados de ideas afines para disuadir las actividades informáticas maliciosas contrarias a dicho marco.

Estados Unidos y Chile se comprometen a continuar desarrollando una estrecha colaboración en torno a la ciberseguridad, la protección de la infraestructura crítica, de respuesta ante incidentes, la protección de datos, la provisión de tecnologías informáticas y de comunicación, la seguridad informática internacional, y la cooperación militar y entre instituciones de aplicación de la ley a través del establecimiento de canales sólidos para la comunicación abierta en torno a los asuntos informáticos de cuidado.

Marco de trabajo de ciberseguridad del NIST

Historia y antecedentes

Como resultado de la creciente cantidad de ataques informáticos a sistemas de infraestructuras críticas y al impacto que dichos ataques pudieran tener en el contexto de la seguridad nacional de Estados Unidos, el 12 de febrero de 2013 el Presidente Barack Obama redactó la Orden Ejecutiva (EO) de Mejora de Ciberseguridad de Infraestructuras Críticas (Executive Order 13636 -- Improving Critical Infrastructure Cybersecurity) en donde se delegaba en el NIST (National Institute of Standards and Technology) el desarrollo de un marco de trabajo para la reducción de riesgos asociados con este tipo de entornos, con el soporte del Gobierno, la industria y los usuarios.

Marco de trabajo de ciberseguridad del NIST

El resultado de este trabajo - posterior a la publicación de múltiples versiones preliminares y recepción de contribuciones de voluntarios a través del modelo de Request for Information (RFI) – fue la primera versión del documento “Framework for Improving Critical Infrastructure Cybersecurity”, conocido como “NIST Cybersecurity Framework” , que se publicó el 12 de febrero de 2014.

Es de anotar que esta iniciativa no es pionera en su campo. Desde mucho tiempo antes, la OTAN (a través del Centro de Excelencia de Ciberdefensa Cooperativa – CCDCOE) ya había desarrollado una serie de manuales orientados hacia la protección de infraestructuras críticas para la defensa nacional, como es el caso del “Manual del Marco de Trabajo de Ciberseguridad Nacional” (National Cyber Security Framework Manual) publicado en 2012 . Igualmente, ISO/IEC con su estándar ISO/IEC 27032:2012 “Information technology -- Security techniques -- Guidelines for cybersecurity” había sentado un precedente en la definición de guías para la mejora de ciberseguridad. Esto no quiere decir que el marco de trabajo de ciberseguridad del NIST excluya estos documentos, al contrario, los complementa y mejora.

INFORMACIÓN DE CONTACTO

silvas_cr@hotmail.com

Ministerio Secretaría General de la Presidencia

Gobierno de Chile

CHILE LO HACEMOS TODOS

¡Gracias por su Atención!

SEMINARIO CAIGG 2018

Ministerio Secretaría General de la Presidencia