Ministerio de Defensa

Instituto Universitario Aeronáutico
Facultad de Ingeniería

SeminarioRegional de Ciberdefensa

Mgter. Ing. Eduardo Casanovas

Dir. Especialización en Seguridad Informática

Facultad de Ingeniería - IUA

CiberSeguridad
un problema para no dejar escapar

Introducción

Marco Normativo

Sistema Radar

- CiberAtaques
- Vulnerabilidades-Impacto-Mitigaciones

Conclusiones

Introducción

- La afirmación / pregunta con la que da comienzo esta presentación es:

Introducción

- Cyber Security

El presidente Obama ha declarado que "**La amenaza cibernética es uno de los desafíos económicos y de seguridad nacional más serios que enfrentamos como nación**" y que "la prosperidad económica de Estados Unidos en el siglo XXI dependerá de la seguridad cibernética."

Fuente: http://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Introducción

Indicios,.... que demuestran que esta guerra ya comenzó

Introducción



Introducción

Introducción

Marco Normativo y Regulatorio Nacional e Internacional

2001	Nov	Se Firma el primer Convenio Internacional sobre Cibercrimen	Estados miembros del CONSEJO DE EUROPA	Ciudad de Budapest
2005	Abril	Se aprobó los Lineamientos Estratégicos que deberán regir el Plan Nacional de Gobierno Electrónico	Decreto Nº 378/05 del Poder Ejecutivo Nacional	Ciudad de Buenos Aires
2008	Ene a Jul	Se realiza la revisión del articulado de la Convención de Budapest	Personal del MINISTERIO DE RELACIONES EXTERIORES, COMERCIO INTERNACIONAL Y CULTO,	Ciudad de Buenos Aires
2008	Junio	Se sancionó la Ley Nº 26.388 por la cual se modificó el CODIGO PENAL (Ley de Delitos Informáticos)	Congreso Nacional	Ciudad de Buenos Aires
2010	Marzo	Argentina solicita la adhesión al convenio de Budapest	CONSEJO DE EUROPA	Ciudad de Estrasburgo
2011	Julio	Se crea El Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad	Resolución 580/2011 JEFATURA DE GABINETE DE MINISTROS	Ciudad de Buenos Aires

Marco Normativo y Regulatorio Nacional e Internacional

2011	Sep	Se aprueba el “FORMULARIO DE ADHESION AL PROGRAMA NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACION Y CIBERSEGURIDAD”	Disposición 3/2011 Oficina Nacional de Tecnologías de Información	Ciudad de Buenos Aires
2011	Oct	Se crea una Comisión Asesora de Cibercrimen	Resolución Conjunta 866/2011 y 1500/2011 Jefatura de Gabinete de Ministros y Ministerio de Justicia y Derechos Humanos	Ciudad de Buenos Aires
2012	Marzo	Declaración “Fortalecimiento de la Seguridad Cibernética en las Américas”	El Comité Interamericano contra el terrorismo (CICTE) perteneciente a la Organización de los Estados Americanos (OEA)	Ciudad de Washington, D.C.
2013	Ago	Se crean 4 Grupos de Trabajo “ICIC - CERT” (Computer Emergency Response Team), “ICIC - GAP” (Grupo de Acción Preventiva), “ICIC - GICI” (Grupo de Infraestructuras Críticas de Información), “ICIC - INTERNET SANO”	Disposición 2/2013 Oficina Nacional de Tecnologías de Información	Ciudad de Buenos Aires
2013	Ago	Se aprueba la “Política de Seguridad de la Información Modelo”.	Disposición 3/2013 Oficina Nacional de Tecnologías de Información	Ciudad de Buenos Aires

Sistema Radar

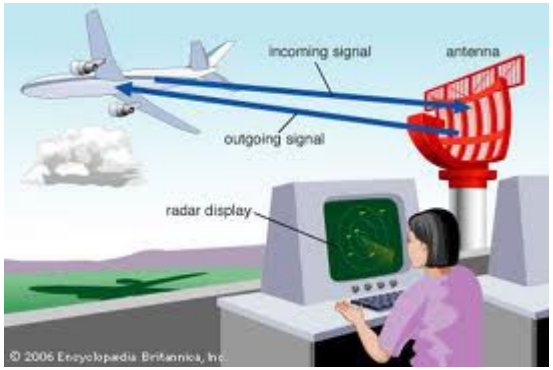
Siendo la ciberseguridad el tema que pretendo desarrollar, es importante analizar donde debemos ubicar nuestras barreras defensivas.

Entonces pensemos como está compuesto un Sistema Radar.

Sistema Radar

Antes de realizar una **evaluación de riesgo para detectar potenciales vulnerabilidades**, se debe entender el funcionamiento global del sistema.

Distintos sistemas requerirán distintas soluciones



Sistema Radar

Ciberataques

- Sep 2007 **aviación israelí atacó instalaciones nucleares Sirias.** La Fuerza Aérea Israelí fue capaz de penetrar con sus aviones de combate en el **Espacio Aéreo Sirio sin ser detectados por radar.** Este sistema permitió manipular directamente la señal recibida por los radares enemigos, mostrando en sus sensores objetivos falsos.
- Hacia finales de 2010, varios informes sugirieron que durante un **ejercicio militar iraní, seis señales no identificadas de aeronaves aparecieron en su sistema,...** y aviones de combate fueron enviados para interceptar a lo que se presumía eran aviones enemigos.

Sistema Radar

Ciberataques

- Sin embargo, una vez en el aire todo lo que se encontró fue el espacio aéreo vacío. Se especula que fue el mismo virus **Stuxnet** que había afectado a la industria nuclear de Irán y los sistemas militares se había infiltrado en su radar militar.
- En 2011 durante los **ataques aéreos contra el régimen de Gadafi en Libia** , se decía que los funcionarios de la administración de Obama habían considerado **hackear los radares de alerta temprana** para ocultar el acercamiento de los aviones de ataque. A pesar de la confianza que se tenía en el código de ataque, el método se considera un paso de último recurso que no se empleó en este caso. Sin embargo, si las circunstancias asi lo indicaban, había especialistas del Cyber Command listos para realizarlo.

Sistema Radar

Ciberataques

- En 2014 la desaparición del vuelo MH370 de Malasya Airlines, **fue un ciberataque?**
- Frente a la falta de autenticación de **la señal del transponder, pudo esta haber sido reemplazada por otra para ocultar el verdadero momento y lugar de la desaparición?** Es posible clonar la señal de un transponder?
- Fueron los radares de tierra engañados con señales falsas?

Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

Podemos determinar tres grandes **puntos vulnerables.**

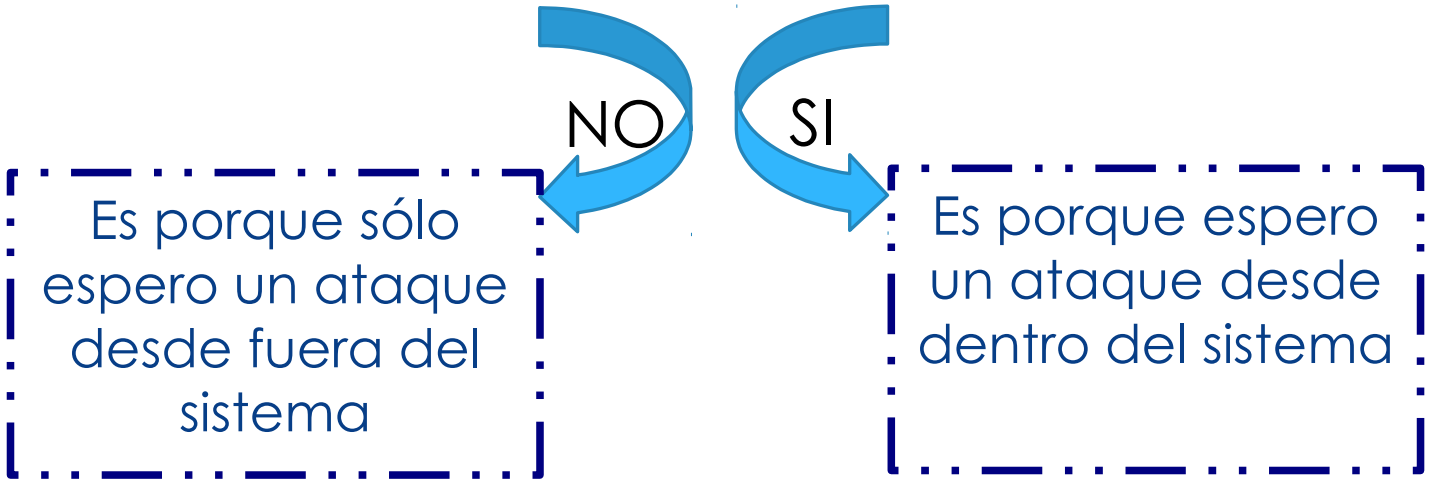
Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

- El sistema debe ser analizado **EXTERMO A EXTREMO**
- El sistema **NO** va a tener acceso a Internet.
- El sistema **puede** ser atacado?



Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

1)El Sistema Radar propiamente dicho.

Además de las contramedidas electrónicas que posee el equipo y que busca mitigar los ataque conocidos.

RS

Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

1) **El sistema Radar propiamente dicho**

Una muestra que el sistema es vulnerable son los **virus como Stuxnet o Flame.** Debemos analizar si los mismos ingresaron al sistema **desde dentro o desde fuera del mismo.** Dicho análisis nos posiciona en puntos totalmente diferentes y con metodologías de defensa también diferentes

Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

2) El Sistema de Comunicación

Debemos analizar los vínculos y tipos de enlace que se tienen entre los sensores y el centro de procesamiento.

Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

2)El Sistema de Comunicaciones

No en todos los sistemas de radar encontramos un sistema de comunicaciones pero en aquellos en los que sí tienen los mismos deben ser cuidadosamente analizados debido a que, **si las señales no se transmiten protegidas con métodos de encripción y autenticación** , pueden ser atacadas y modificadas

Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

3) La Red.

Sistema Radar

Vulnerabilidades – Impacto - Mitigaciones

3) La Red

Debido al uso de **protocolos estándares de comunicación y transporte, se está expuesto a la interceptación y modificación del tráfico.** Es por eso que es mandatorio que el 100% del tráfico que se realice entre los distintos terminales y puestos de trabajo, sea por medio de un **protocolo seguro.**

Sistema Radar

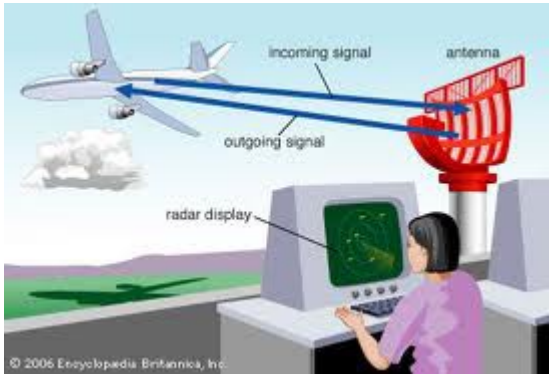
Vulnerabilidades – Impacto - Mitigaciones

Activo	Tasación	Factor de Riesgo	Ponderación Ocurrencia	Prob del Riesgo (%)	Nivel de Vulnerabilidad
Servi-dores	8	Corte de luz, UPS descargado o variaciones de voltaje	1	14,29	_114.32
		Destrucción o Mal funcionamiento de un componente	1	14,29	_114.32
		Errores de configuración y operación	1	14,29	_114.32
		Factores Ambientales	1	14,29	_114.32
		Mal mantenimiento	2	28,57	_228.56
		Robo	1	14,29	_114.32
		Virus, Gusanos y Caballos de Troya	3	43,26	_343.28
		Cant de Factores de Riesgo	7	_143.28	_1143.04

Sistema Radar

Vulnerabilidades – **Impacto** - Mitigaciones

Estudio y evaluación de las pérdidas y daños sufridos despues de un ataque.



Las diferentes vulnerabillidades generan diferente tipo de impacto.

Sistema Radar

Vulnerabilidades – **Impacto** - Mitigaciones

Es necesario realizar un clasificación **cuantitativa** y **cualitativa** del impacto generado por cada vulnerabilidad detectada.

Sistema Radar

Vulnerabilidades – **Impacto** - Mitigaciones

El impacto en terminos de la perdida del control del tránsito aéreo puede llegar a consecuencias muy graves.

- Ejemplo: Sistema de comunicaciones
- Incidente: Se produce un ataque DoS en el uplink Cba-Ezeiza
- Impacto: Perdida de información de las aeronaves que sobrevuelan el sector

Sistema Radar

Vulnerabilidades – Impacto - **Mitigaciones**

Son **medidas tomadas con anticipación** con el ánimo de reducir o eliminar el impacto.

Incluye tanto la **planificación** como la **ejecución** de medidas y el proceso de planificación para una respuesta efectiva ante los desastres que ocurran.

Sistema Radar

Vulnerabilidades – Impacto - **Mitigaciones**

Sistema Radar

Vulnerabilidades – Impacto - **Mitigaciones**

Si vemos como se han manifestado los ciberataques a los sistemas, los mismos han buscado de ocultar señales existentes o bien generar señales que simulen la existencia real. Y esto se debe a que **una vez que la señal pudo ser inyectada no hay forma de validar la autenticidad** de la misma, es allí donde radica una de las claves para hacerle las cosas más complicadas al atacante.

Sistema Radar

Vulnerabilidades – Impacto - **Mitigaciones**

1)El Sistema Radar propiamente dicho

- Las mitigaciones de los riesgos a los que está expuesto el sistema **sólo van a ser efectivas si se piensan en forma global.** Es decir, que la seguridad es un problema integral **– End to End –** y como tal, debe entenderse que no sirve asegurar el 90% del sistema porque el atacante descubrirá el 10% que no ha sido asegurado y sobre eso va a actuar. **Por definición el atacante va a ir por el punto más débil.**

Sistema Radar

Vulnerabilidades – Impacto - **Mitigaciones**

- Otro aspecto a la hora de plantear mitigaciones, es que **NO todas son técnicas ya sea de software o de hardware.**
- **Los usuarios del sistemas son partícipes necesarios** que deben ser tenidos en cuenta y sobre los cuales recae todas las recomendaciones y buenas practicas de un sistema informático.

Sistema Radar

Vulnerabilidades – Impacto - **Mitigaciones**

CybAIR Radbox

Actualmente ya hay sistemas desarrollados que tienen incorporados diferentes medidas de seguridad que intentan mitigar las vulnerabilidades conocidas

Conclusiones

- Ya no es una pregunta sino que es una afirmación **"La CiberGuerra** ya comenzó."
- Cuando hablamos de **ciberseguridad,** necesariamente debemos considerar las acciones que se van a desarrollar para **proteger** de manera coherente y sistemática **los activos de información crítica**, distribuidos en toda su infraestructura.
- Sólo haciendo un **análisis exhaustivo de las vulnerabilidades** se puede generar la mitigación necesaria para cada una de ellas.
- **Reaccionar frente a un ataque** de denegación de servicio o rechazar una intrusión etc., son algunos de los retos que el entorno digital nos plantea.
- El **Sistema de Radar** como alerta temprana o como control aéreo no puede quedar al margen de este análisis porque es de fundamental importancia en nuestro desarrollo como Nación .

Conclusiones

Gracias por su atención

Reflexión

Este nuevo escenario bélico plantea necesidad de tomar nuevas decisiones:

- **conformar nuestra Fuerza de Ciberataque** o solamente
- **preparar nuestras Ciberdefensas** adecuadamente
- ... será que la tendencia planteada para el 2014 de **Militarización del Ciberespacio** nos va a enfrentar a esta disyuntiva,....
- **cuánto falta para que nuestra continuidad como Nación libre y soberana nos obligue a dominar nuestro entorno digital,....**

Back Up

Requerimientos de seguridad????

- 1) El cuadro de texto de “Login” debe tener un boton de “Olvidó su contraseña”
- 2) El cuadro de texto de “Login” debe tener un boton de “Obtenga un usuario”

Follow TCP Stream

Stream Content

```
POST /homebanking/LoginSubmit.do HTTP/1.1
Host: ihbl[redacted].com.ar
Connection: keep-alive
Content-Length: 422
Cache-Control: max-age=0
Origin: http://ihbl[redacted]com.ar
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/535.2 (KHTML, like Gecko) Chrome/15.0.874.121
Safari/535.2
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://ihbl[redacted].com.ar/homebanking/display.jsp?body=login/login.jsp
Accept-Encoding: gzip,deflate,sdch
Accept-Language: es-ES,es;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: Persistence_Cookie=252843692.47873.0000; JSESSIONID=0000NrFta5l2FzlDtEXC9OCno0Q:-1

tecladoOn=&navegador=Navegador%3A+Netscape+version%3A+5.0+%28Windows+NT+6.1%3B+WOW64%29+AppleWebKit%2F535.2+%28KHTML
%2C+like+Gecko%29+Chrome%2F15.0.874.121+Safari%2F535.2+plataforma%3AWin32+UserAgent%3A+Mozilla%2F5.0+%28Windows+NT
+6.1%3B+WOW64%29+AppleWebKit%2F535.2+%28KHTML%2C+like+Gecko%29+Chrome%2F15.0.874.121+Safari%
2F535.2&tipodoc=&documento=9879827&usuarioHB=roberto12&password=12345678&Ingresar.x=22&Ingresar.y=7HTTP/1.0 200 OK
Date: Tue, 29 Nov 2011 08:04:09 GMT
Server: IBM_HTTP_SERVER
Pragma: no-cache
Cache-Control: no-cache
expires: -1
Content-Type: text/html;charset=ISO-8859-1
Content-Language: es-AR
```

Requerimientos de seguridad

- 1) El campo “Usuario” y “Contraseña” deben ser transmitidos encriptados o hasheados
- 2) La interfaz de ususario no debe permitir un ataque XSS o HTML inyección en todos los text box en los que el usuario tiene acceso

Stream Content

```
...X..z.....*(..!...6.z.....Vv..q...H&n'...m....y2._.M.0.}%X..B.[...4..|zY....J...<....dM
{.'.Lb .8../...y.6%.N.........EFk@..9.-..lC...A$.?D.L...@..aj.I..G.Z..X5.2.LEt0]4.........../
j ..he.............1._8..........).............0T...}^..0:.....|.B:....m|..\.k..........pX....$.V..K.A..#.F..'%
0...|.....K..r.n............wYa.........$G.H...lC.....ld.."}.../e.`t.......w7!M3i.Z..J.....W]ZG..7.M..wLNQ.}
HY..;..szF-..D.;..L.kI.i*....5.</.....d.m.W|j)..F...~..Hn+....3B....'.
.....:.s.W..(.....=.....S.....=..T....>..!.<7...
CH.p..C....f..Q.%B..B....3...J...
y.=....
x...'.....J>F..q..`...<.6*...N..2....|=..z.....RL...o.I.....7...
(..Q.F......*.....9.........L.Bt.......3..Y.....i..0..........z...kG..d\n.Bv....,]$......5Z....S....U.y.
%...!........!...Jq;.b.Jq}De.H -Jj..h.B.
.
bN 7q..9MD.Y.r/...W-....Fc....T..Ny...f.........,E..AGO....v..3t\,...b..m.....l.;~*"....:."RCo.(V.r.I.y..e<%
$!.......Y..G.O....dl.L%.e5.;X!c..E.d.K.l/49......?J..).M..L..B..L..k....E....u8.N..._._....x.G.....KW.n;.g.c...h.]
5....^..2Y....^.....|Y...F..D.....x...)~;...)...C.2/.Y}...tB.
.D..>}.......ZY.x`...'....I>./ )...D..c.Mon..V.......-..B...f../....;...d.da\....n..f...7D....Wk:V..4....j?
$9T.K.4d.......E..>....k..^J.v...g..0.S=..,l.....Z?8..z|
u.v'...r.9...'..... .........c.cX.....&.9.......PG ..7_....X.u..:.(.,p!.D]Z.s9L,=C.AZ(>M.t.%..S.l!:....Eu.z.
.=...+#.Y.....PX..8.]n.]....0..a.;
.v.2...h.......-.....,qi.x;...%..p.)..(..Z...W~.\t9.{:...
p....8.{\W.o.S...uw...6..f.....d....[..g.......<.ky....Q.....l..d?..$W.q.2.@.....9.........@B....ZoU....g.......
(..'Is.+.......~.k.{..4......".........&.v.u.o:.
.?...g.~.r.kY7O.g....E.c^.@Z.8Xl\.W
.....?.OXIw.b.+.'...DK.{..Pp..($..5.JO...`-.z....|AI9^Q.2.H..D..27...O
.o..Z...8...O.U.....m...k).lRHD..b.....+.IZ..R.^....U&....P...!..#...$.H.<c<../U....m.B.P$...u....Q .......U.>.?.
+..e.......DJ.DK..+Q.nu@...R..x.Q.....]C.a....m-.....;..b.-0T..$.-...
O.....{./.....6.r.....RW._.k..E..hI].....
..U3~.F.l...|.'Y....;I..A.k.........9~."....!d
\u.q....{;We..s.J.....8 ...3*K...C'..].........T.a...f...q;........s J....a....G..|.>..[...
```

Find | Save As | Print | Entire conversation (4173 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | R

Help | Filter Out This Stream | Close

Ra