XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectivas

CCN-CERT
centro criptológico nacional

- Antonio GrimaltosVidal
- Oficina de Seguridad de la Información (OSI)
  Conselleria de Sanitat Universal i Salut Pública
  Generalitat Valenciana
- grimaltos_ant@gva.es
- @Agrimaltos

Índice

La conexión a la red de todo tipo de dispositivos ha supuesto una revolución tecnológica y social representada fundamentalmente por el paradigma de “Internet de las Cosas” (IoT), en el que multitud de dispositivos son capaces de interaccionar entre sí a través de Internet y proporcionar así servicios de valor añadido a los usuarios.

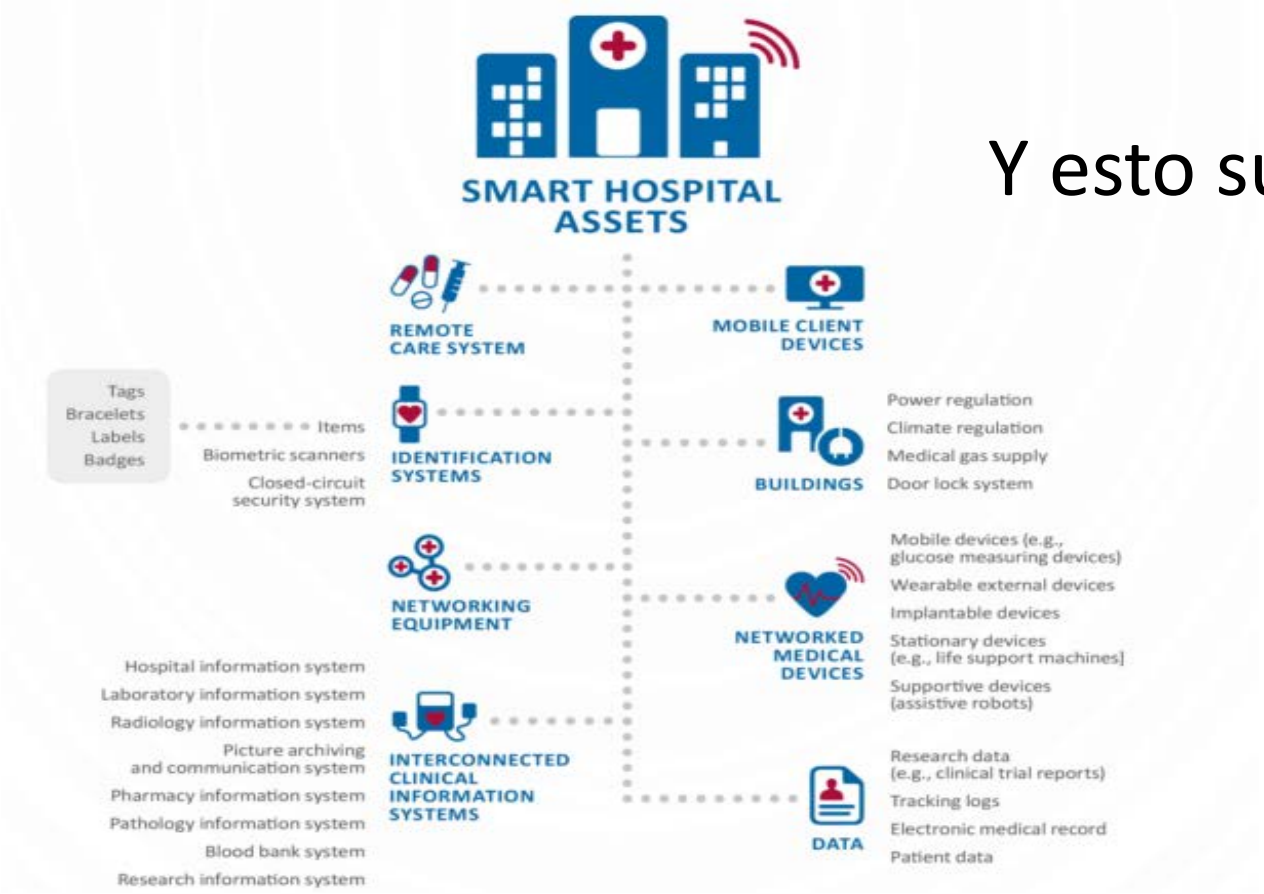
El Sector de la Salud y los Servicios sanitarios no está ajeno a esta revolución.

Pensemos en los dispositivos que se utilizan en los Centros sanitarios:

- Grandes máquinas de diagnóstico
- Dispositivos de monitorización de soporte vital
- Pequeños sensores móviles
- Equipos, (fijos o móviles), utilizados por los profesionales sanitarios en su trabajo diario.

No podemos olvidarnos, también, de una gran cantidad de dispositivos que, aun no siendo dispositivos médicos, si contribuyen a garantizar la adecuada provisión de servicios médicos:

- Dispositivos asociados a sistemas de climatización
- Sensores anti-incendios
- Dispositivos de control de acceso a zonas restringidas.
- Etc,…



Y esto supone …

… Añadir un riesgo.

IoT en general es sinónimo de poca seguridad

- Casi todo lo relacionado con la **IoT**, recopila datos durante el uso y, a menudo, comparte esa información con sus fabricantes sin que los usuarios sepan **que es lo qué** se está recopilando.
- En muchos casos, las funciones del producto dependen de la conexión a Internet.
- Los fabricantes de todo tipo de dispositivos electrónicos o eléctricos se apresuran a agregar funciones que requieren conexión a Internet.
- En su prisa por comercializar, pasan por alto las complicaciones del diseño y la construcción de seguridad de hardware y software debido a las "prisas" por obtener la función más nueva y más "fresca" al menor coste.

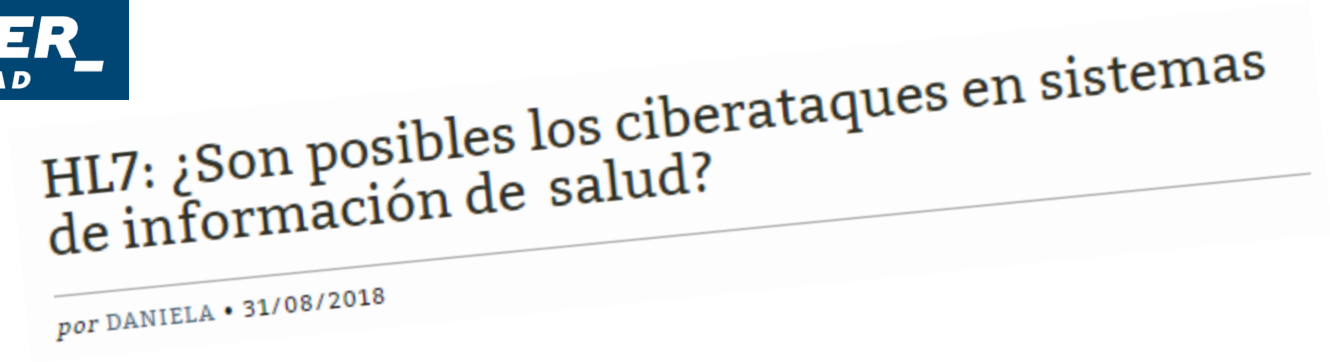
Hackear un marcapasos es posible (y Cheney lo sabía)

Matar a alguien con marcapasos es posible para un buen hacker informático. Eso es algo que hemos visto en la ficción pero que el que fuera vicepresidente con Bush supuso y se adelantó pidiendo que quitaran el WiFi a su dispositivo.

HL7: ¿Son posibles los ciberataques en sistemas de información de salud?

por DANIELA • 31/08/2018

Un grupo de médicos y expertos en informática de la Universidad de California ha demostrado **con facilidad que es posible modificar de forma remota los resultados de las pruebas médicas de los pacientes a través de un ataque a la conexión que existe entre los dispositivos médicos de laboratorio y los sistemas de registros médicos.**



HL7: ¿Son posibles los ciberataques en sistemas de información de salud?

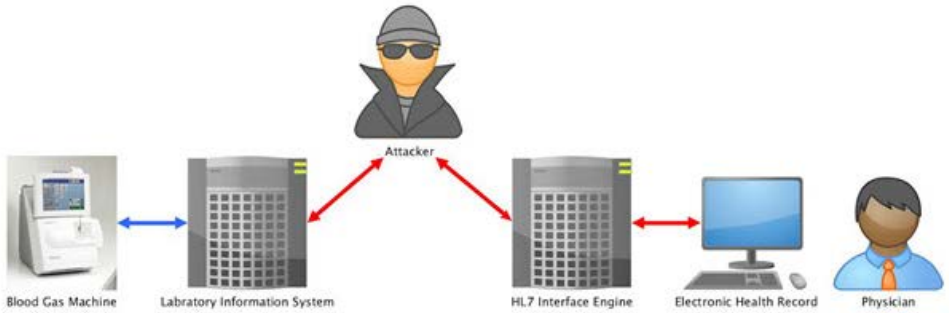
por DANIELA • 31/08/2018

Los estándares del Nivel de Salud 7 o HL7, los cuales son usados para la transferencia de datos de pacientes dentro de redes hospitalarias, son los principales detonantes de estas vulnerabilidades.

En concreto, es el lenguaje HL7 el que puede ser aprovechado por los hackers, el mismo que hace posible la comunicación entre todos los dispositivos y sistemas de comunicación en una instalación médica, **y fue desarrollado en la década de 1970 sin mayores cambios de seguridad informática hasta la fecha.**

https://youtu.be/k6ovFgIZ9nw

Los investigadores utilizaron un 'ataque de hombre en el medio', a través del cual lograron automatizar el proceso para obtener el control de los datos de forma remota. En vez de infiltrarse en el sistema médico existente, los expertos construyeron un banco de pruebas compuesto por dispositivos de pruebas de laboratorio médicos, ordenadores y servidores.



Esto les permitió realizar pruebas como análisis de sangre y de orina, interceptar los resultados de laboratorio, modificarlos y luego enviar estos datos a un sistema de registros médicos.

¿Por qué nos quita el sueño pensar en estos dispositivos?

Las principales razones por las que los dispositivos médicos se conectan tanto a la red Local como a Internet son:

1. La compartición de información entre servicios.

   La radiografía hecha por un equipo (IoT) a un paciente se puede consultar en un servicio especializado o en una consulta de un ambulatorio.

2. La seguridad de los pacientes.

   Los dispositivos conectados a la IoT alertan a los fabricantes, a los técnicos etc…, sobre equipos defectuosos o que funcionan mal.

3. El ahorro de costes

   Esta conexión permite ver y planificar las necesidades de mantenimiento, incluso permiten ajustes en remoto.

Vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza.

Una pequeña reflexión

Una vulnerabilidad en un equipo de electro medicina puede ser aprovechada para cambiar su funcionamiento, provocar daño al paciente e incluso robar datos que formen parte de una investigación pero la especialización que se requiere para efectuar este tipo de ataque hace que la probabilidad de que se produzca en estos términos sea muy baja, aunque el impacto de este incidente produzca un daño irreparable,

Vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza.

Una pequeña reflexión

Una vulnerabilidad en un equipo de electro medicina puede ser aprovechada para cambiar su funcionamiento, provocar daño al paciente e incluso robar datos que formen parte de una investigación pero la especialización que se requiere para efectuar este tipo de ataque hace que la probabilidad de que se produzca en estos términos sea muy baja, aunque el impacto de este incidente produzca un daño irreparable, pero …

además puede ser aprovechada esta vulnerabilidad para ser un punto de entada a la red corporativa, y con ello, poder propagarse al resto de equipos, ex filtrar datos, robar credenciales, cifrar y pedir un rescate, conseguir miembros de una botnet, etc…

A medida que la tecnología mejora**, mejora la calidad** de los servicios que prestamos **pero, los vectores de ataque aumentan**, y por tanto **los riesgos aumentan.**

Los ataques a la IoT exponen a las empresas a la pérdida de datos y servicios y pueden hacer que los dispositivos conectados sean peligrosos para los clientes, empleados y para el público en general. Las potenciales vulnerabilidades seguirán creciendo a medida que más dispositivos sean dependientes de Internet.

La mayoría de **los dispositivos IoT no se diseñan ni construyen teniendo en cuenta la seguridad propia y la de otros**, sino que son diseñados en pro de la funcionalidad, su facilidad de uso y su rápido lanzamiento al mercado.

Se denomina riesgo a la incertidumbre sobre lo que puede pasar. (Guía CCN-STIC 470-I1)

¿Como nos enfrentamos a esos nuevos riesgos?

Se denomina riesgo a la incertidumbre sobre lo que puede pasar. (Guía CCN-STIC 470-I1)

¿Como nos enfrentamos a esos nuevos riesgos?

GOBIERNO DE LA SEGURIDAD

Se denomina riesgo a la incertidumbre sobre lo que puede pasar. (Guía CCN-STIC 470-I1)

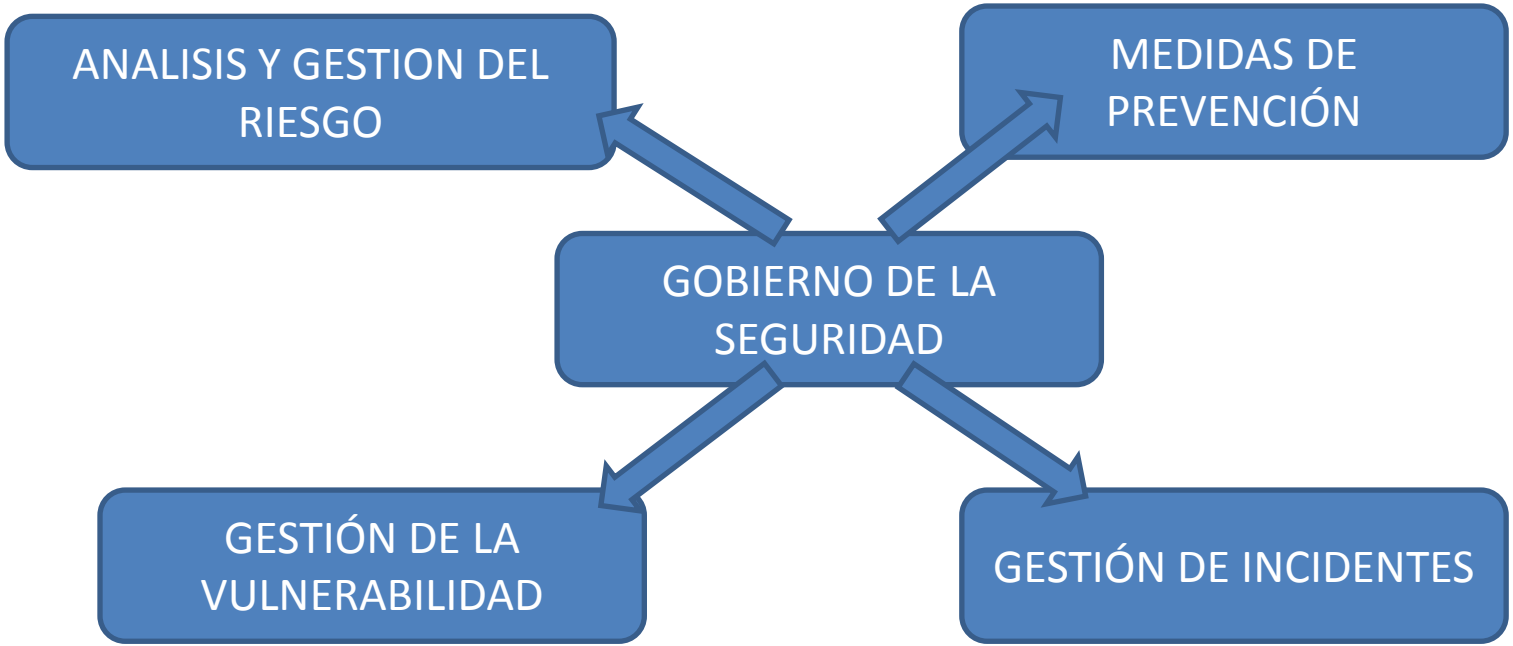
¿Como nos enfrentamos a esos nuevos riesgos?

Artículo 4. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

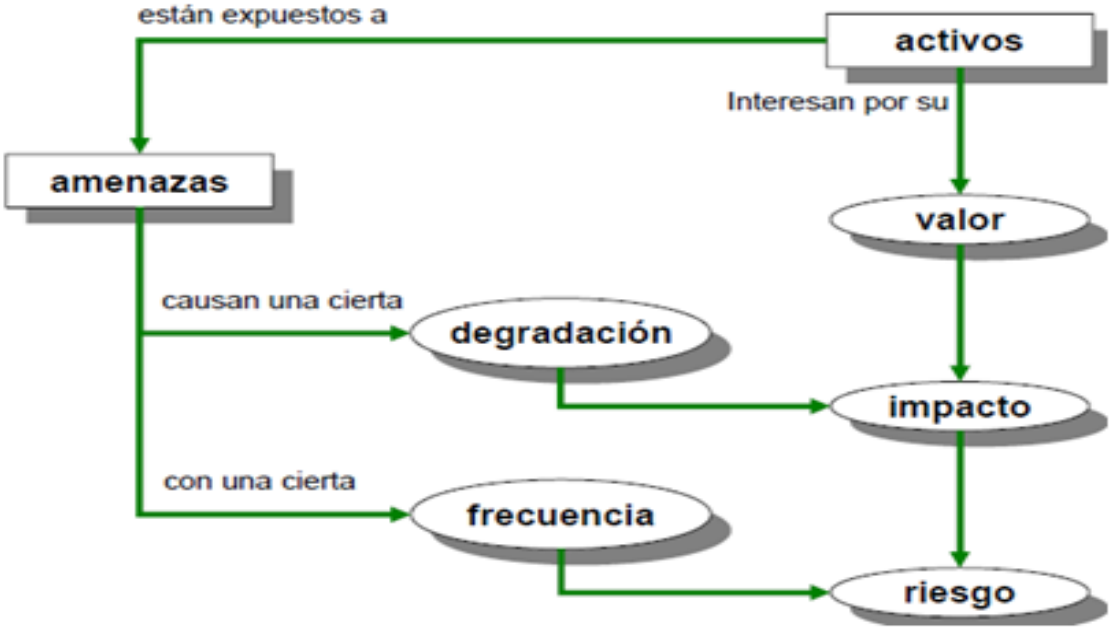
a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada

b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.



ANALISIS Y GESTION DEL RIESGO

Este principio básico se desarrolla en el ENS en los Artículos 6 y 13, aunque esta presente a lo largo de la filosofía de todo el ENS.



Artículo 6. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá **un equilibrio entre** la naturaleza de los datos y los tratamientos, **los riesgos a los que estén expuestos y las medidas de seguridad.**

Artículo 13. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.
2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.
3. **Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.**

Artículo 6. *Gestión de la seguridad basada en los riesgos.*

.

... La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá **un equilibrio entre** la naturaleza de los datos y los tratamientos, **los riesgos a los que estén expuestos y las medidas de seguridad.**

Artículo 13. *Análisis y gestión de los riesgos.*

.

Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Se denomina riesgo a la incertidumbre sobre lo que puede pasar. (Guía CCN-STIC 470-I1)

El análisis de riesgos proporciona información para decidir sobre la asignación de recursos, ya sean técnicos o de otro tipo, para proteger organización. Y además, requiere un enfoque metódico:

1. Identificar el valor que hay que proteger
2. Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño,
3. Establecer medidas de seguridad para protegernos contra los ataques y
4. **Estimar indicadores de la posición de riesgo para ayudar a los que tienen qué tomar decisiones.**

Tomemos un ejemplo

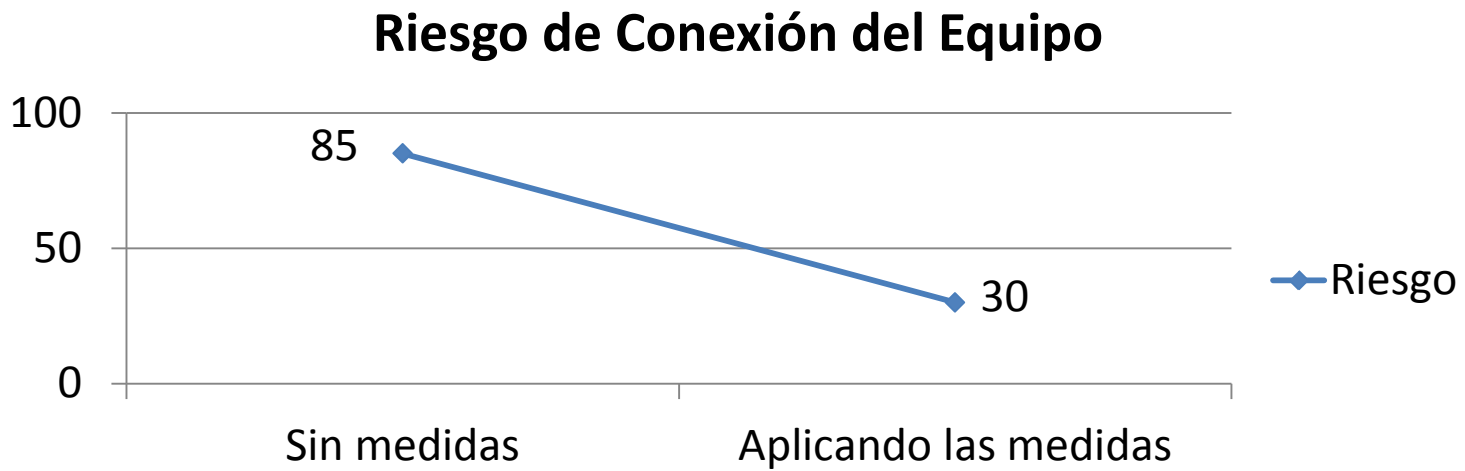
Por necesidades del servicio de cardiología, ya que hay un pico de trabajo en ese servicio, necesitamos poner operativo un equipo de electrocardiogramas, cuyo S.O. es XP.

1. Identificar el valor que hay que proteger.
   - Los datos recogidos por el equipo que afectan a la salud de un paciente, su gravedad, tratamiento, etc…
2. Identificar los elementos del sistema que soportan ese valor; es decir, aquellos donde los ataques pueden causar daño,
   - El equipo esta en la red corporativa ya que se le ordena el trabajo desde el servicio correspondiente y accede a la base de datos donde se guardarán los datos referidos a dicho estudio.
3. Establecer medidas de seguridad para protegernos contra los ataques y
   - Actualizar el S.O antes de ponerlo operativo.
   - Actualizar el antivirus.
   - Solo acceso a la red interna (a la externa solo si es absolutamente necesario).
   - Vigilancia específica en el IDS.
4. Estimar indicadores de la posición de riesgo para ayudar a los que tienen qué tomar decisiones.

Tomemos un ejemplo

Por necesidades del servicio de cardiología, ya que hay un pico de trabajo en ese servicio, necesitamos poner operativo un equipo de electrocardiogramas, cuyo S.O. es XP.

4. Estimar indicadores de la posición de riesgo para ayudar a los que tienen qué tomar decisiones.



Tomemos un ejemplo

Por necesidades del servicio de cardiología, ya que hay un pico de trabajo en ese servicio, necesitamos poner operativo un equipo de electrocardiogramas, cuyo S.O. es XP.

[OSI] INC-903329 NUEVO: Alertas de Malware en el informe diario del 26/09/2018 referidas a actividad del 25/09/2018, 1040 alertas

SDGSISServicedesk@gva.es

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Enviado: miércoles 26/09/2018 10:12
Para: grimaltos_ant@gva.es

ANTONIO SERVICIOS CENTRALES

Tipo	Estado	Prioridad	Fecha Apertura	Ticket padre	Ticket sistema externo
Incidente	Asignado	3	26/09/2018 10:07:53		

Asignatario	Grupo	Aplicación Afectada	Módulo funcional	Entorno
GRIMALTOS VIDAL, ANTONIO	OSI			PRO

Nº Serie	Nombre	IP	Modelo	Fabricante

Suscrito1	Suscrito2	Suscrito3	Suscrito4

Descripción del ticket

En el informe de alertas aparecen, 1040 alertas relacionadas con la IP:

172.17.87.79

Según arterias esta en vuestro ámbito,

Id: 2090
IP de red: 172.17.84.0
Máscara de red: 255.255.252.0
Nombre: USR2
Nodo: [redacted]
VLAN: USR
Descripción:

Según hemos hablado es un equipo en XP que se ha conectado por necesidades del servicio. mira más información y os la envío.

Echad un vistazo y nos decís algo.

Para mayor información, pulse: http://servicedesk.san.gva.es:8080/CAisd/pdmweb.exe?OP=SEARCH+FACTORY=iss+SKIPLIST=1+QBE.EQ.id=1302456

1040 Alertas

Lecciones aprendidas….

Del 26/09/2018
Al 20/09/2018

Conexión equipo Hospital [redacted]

[redacted]

Enviado: martes 20/11/2018 17:20
Para: avs.alertas.seguridad@gva.es
CC: lafe.alertas.seguridad@gva.es

Buenas tardes,

Hemos conectado a la red un pc clínico de monitorización de pacientes que se utiliza esporádicamente en el servicio de epilepsia del hospital la fe. Está con las definiciones de virus actualizadas pero en ocasiones nos habéis avisado de alguna alerta incluso en ocasiones han sido falsos positivos.
Os indico los datos por si detectáis cualquier actividad sospechosa.

IP: 172.17.87.82

Saludos.

[redacted]

Artículo 7. *Prevención, reacción y recuperación.*

1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
2. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.
3. …/…

La seguridad del sistema debe contemplar … los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, …

- PREVENCIÓN

  ¿Cómo prevenimos que ataquen los dispositivos IOT?

  … No les dejes subir al avión….

- DETECCIÓN
- CORRECCIÓN

- PREVENCIÓN

¿Cómo prevenimos que ataquen los dispositivos IOT?

Tenemos que abordar la cuestión desde **2 puntos de vista**.

1. Acciones sobre los que ya tenemos en nuestros sistemas.
2. Acciones sobre futuros dispositivos.

SEGURIDAD IOT

10/10 Permite '123456'
10/10 No Bloquea
10/10 Permite Enumeración de Usuarios
9/10 no tiene Doble Factor de Autenticación
8/10 Recoge Información Personal
7/10 no usa Cifrado
6/10 Interfaces Vulnerables a XSS/SQLi
SSH a la Escucha
Video Streaming sin Autenticación
Ausencia total de Actualizaciones

How safe are home security systems?
An HP study on IoT security

SEGURIDAD IOT EN SANIDAD ¿ESTAMOS PREPARADOS?

MEDIDAS DE PREVENCION

Acciones sobre los dispositivos IOT que ya tenemos en nuestros sistemas.

- Cambiar claves por defecto.
- Separar los dispositivos por tipos en una VLAN específica para ellos.
- Comunicación con otros dispositivos (PC´s, BBDD) de otras VLAN cifradas.
- Insistir al fabricante en las actualizaciones y en la conveniencia de instalarlas.
- Si el dispositivo se comunica con el propio fabricante, asegurarnos de que las comunicaciones van cifradas.
- Reglas de firewall específicas para la protección (este analizador, con esta IP solo puede enviar trafico de salida hacia esta IP del fabricante)
- Reglas especificas de vigilancia en los IDS o ICS.

Acciones sobre los dispositivos IOT que ya tenemos en nuestros sistemas.

- Cam
- Sep ellos.
- Cor N cifr
- Insi de inst
- Si e nos de que
- Reg r, con esta icante)
- Regl

,… al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema…

Acciones sobre los dispositivos IOT que podemos incorporar en un futuro

Artículo 11. *Requisitos mínimos de seguridad.*

…/…

g) Adquisición de productos.

…/…

Artículo 18. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

Artículo 18. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser empleados por las Administraciones públicas se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del responsable de Seguridad.
2. La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.
3. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto…

ANEXO V

Modelo de cláusula administrativa particular

Cláusula administrativa particular.–En cumplimiento con lo dispuesto en el artículo 115.4 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, y en el artículo 18 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo indicado en la medida op.pl.5 sobre componentes certificados, recogida en el apartado 4.1.5 del anexo II del citado Real Decreto 3/2010, de 8 de enero.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- 4.1.5 Componentes certificados [op.pl.5].

  Solo se aplica en categoría alta

Categoría ALTA

Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

Una instrucción técnica de seguridad detallará

los criterios exigibles.

- 4.1.5 Com

Solo

Categoría A

Se utiliza … nivel
hayan sid … icados
estén rec … ridad
de las Te

Tendrán … tras de
naturale

Una instr

los …

¿Para cuando una IT de seguridad sobre estos criterios?
o más en concreto una regulación, de obligado cumplimiento, en el ámbito de sanidad

Nueva ISO que sobre IoT

Marca de garantía de ISMS forum.

El fabricante /integrador realiza una declaración responsable a cerca de 100 preguntas . las preguntas son concretas sobre las secciones:

Seguridad en el Diseño

Con preguntas tales como : ¿Dispone la organización de un responsable de seguridad o de alguien con dicho rol para el proceso de diseño del producto de IoT en evaluación?

¿Se ha realizado un análisis de riesgo con anterioridad al diseño inicial del producto y en las modificaciones mayores del producto?

Gobierno y Seguridad en el Ciclo de Vida

Con preguntas como:

¿Dispone el producto de un método documentado para la eliminación segura de la información almacenada sobre un usuario en caso de fin de vida útil o de sustitución de soporte/medios?

Hardware/Firmware

Con preguntas tales como:

¿Se verifica mediante un algoritmo criptográfico que el Firmware ha sido firmado por su compañía antes de proceder a su instalación?

Y así con otras secciones tales como: **Gestión y Actualización, Puertos Externos, Autenticación, disponibilidad, cifrado,** etc…

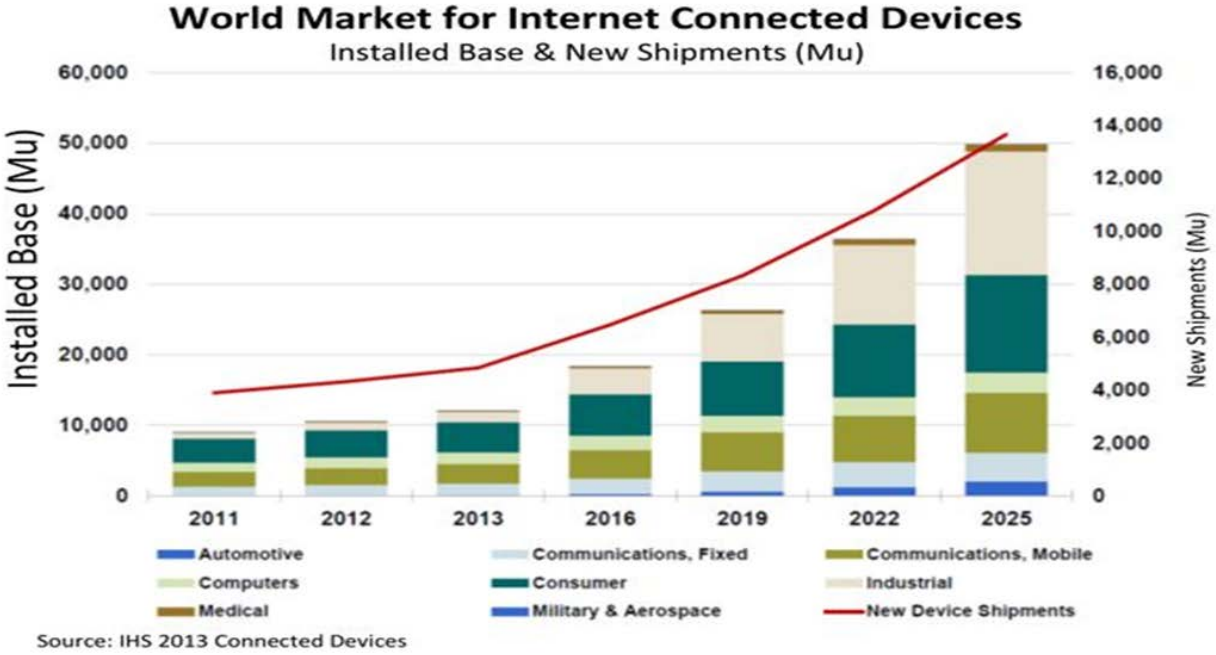
El ISMS se reserva el derecho a auditar en busca de evidencias de cumplimiento o no.

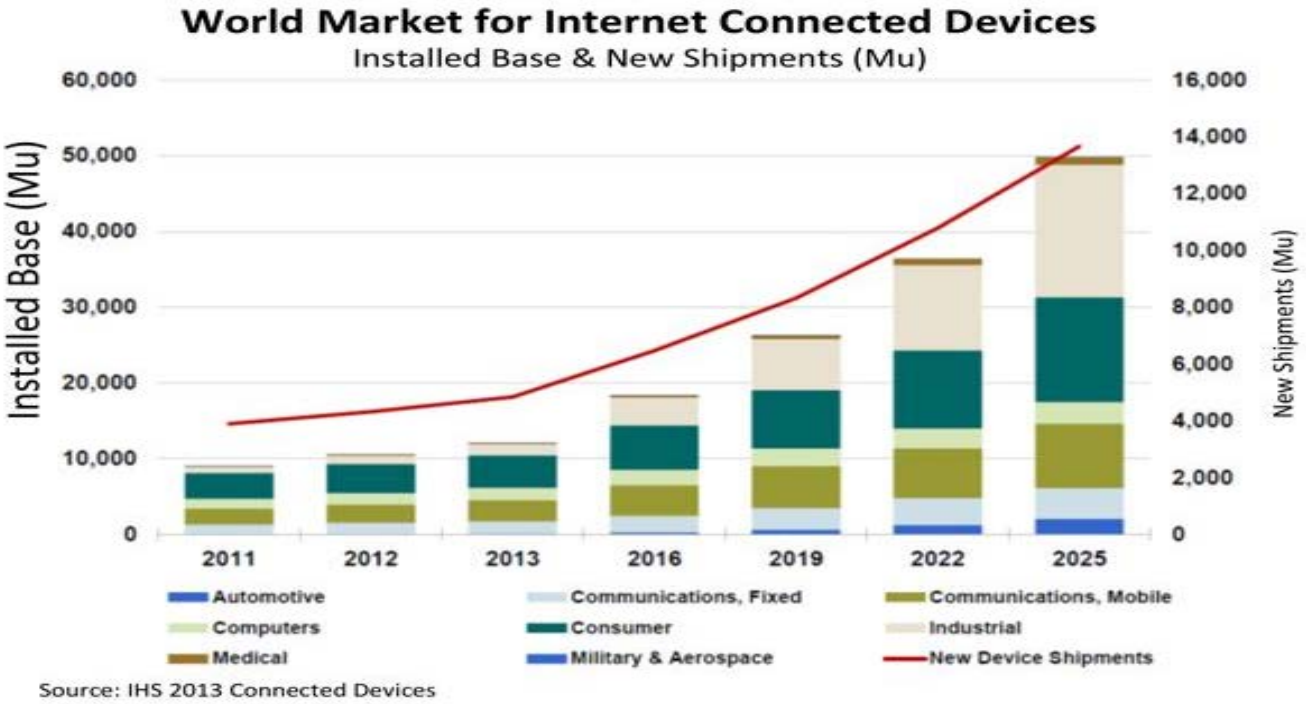
Regulación de IOT del estado de California o de la agencia federal de salud.

Vulnerabilidad es una debilidad que puede ser aprovechada por una amenaza.

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

Según **Gartner**, se espera que la cantidad de dispositivos conectados a Internet alcance los 50 mil millones en 2020. Si bien la IoT mejorará la vida de muchas personas, la cantidad de riesgos de seguridad a los que los consumidores y las empresas se enfrentarán aumentará exponencialmente.





Y como hemos dicho, a mayor numero y variedad de dispositivos, mayor número y variedad de vulnerabilidades.

Artículo 20. *Integridad y actualización del sistema.*

1. …/…
2. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Este conocimiento de las vulnerabilidades (en dispositivos IoT o cualesquiera) y la reacción ante estas para gestionar el riesgo, es algo que esta presente a lo largo de todo el ENS.

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

4.1.1 Análisis de riesgos [op.pl.1].

Categoría ALTA

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

a) Identifique y valore cualitativamente los activos más valiosos del sistema.
b) Identifique y cuantifique las amenazas posibles.
c) <u>Identifique las vulnerabilidades habilitantes de dichas amenazas.</u>

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

4.3.3 Gestión de la configuración [op.exp.3].

Categoría MEDIA y ALTA

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

a) Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).

b) Se mantenga en todo momento la regla de "seguridad por defecto" ([op.exp.2]).

c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).

d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

4.3.4 Mantenimiento [op.exp.4].

Categoría BAJA, MEDIA y ALTA

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.

b) Se efectuará un seguimiento continuo de los anuncios de defectos.

c) Se dispondrá de un **procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.**

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

Categoría MEDIA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de vulnerabilidades.

b) …/…

NECESITAMOS…un

Procedimiento de gestión de la Vulnerabilidad.

Que contemple al menos métodos para:

1. Identificar de posibles vulnerabilidades.
2. Verificar si realmente nos afecta o no.
3. Clasificar la urgencia de corregir esa vulnerabilidad en función del riesgo que corremos y del impacto que produciría en nuestro sistema que se aprovechara esta vulnerabilidad.
4. Conocer quien es el propietario del riesgo y comunicarle la vulnerabilidad.
5. Analizar las posibles soluciones.
6. Probar esas soluciones.
7. Resolver la vulnerabilidad
8. Verificar su resolución.
9. Obtener Conclusiones (Lecciones aprendidas)

La gran Pregunta:

¿Cómo responder ante un incidente de seguridad?

Artículo 24. *Incidentes de seguridad.*

1. Se establecerá un sistema de detección y reacción frente a código dañino.
2. **Se dispondrá de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información. Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema**.

Creo que incluso antes de establecer ese sistema de detección y reacción frente a código dañino, antes deberíamos "prepararnos"

Necesidades para la gestión de incidentes:

1. Formar aunque sea mínimamente al personal del que disponemos y que va a realizar la gestión de incidentes.
2. Documentación de los sistemas y redes que se usan
3. **En el caso de los IoT, Definir cuál es la actividad "normal" para permitir detectar actividades sospechosas que sean indicios de incidentes.**
4. Registrar los contactos de terceras partes.
   - Por ejemplo, si tenemos un servicio que nos da un proveedor, en caso de incidencia hay que tener identificado el responsable en el proveedor. (Directiva NIS), o una garantía en un dispositivo IoT, tener identificado y localizado al servicio técnico
5. Definir una política de gestión de incidentes, así como el procedimiento a seguir en caso de que ocurran.
6. Monitorización lo que ocurre en nuestros sistemas

El procedimiento de Gestión de Incidentes debería contener al menos como realizar las acciones para:

1. Detección y análisis del incidente.
2. Identificación del Incidente.
3. Clasificación y Priorización de Incidentes.
4. Contención Reacción y Recuperación.
5. Recopilación de Lecciones Aprendidas.

DETECCIÓN Y ANÁLISIS

Es evidente que no se podrá gestionar un incidente si éste no se ha detectado.

Los signos de un incidente pueden ser de dos tipos:

Signos indicadores: Son aquellos que ponen de manifiesto que un incidente ha ocurrido o puede estar ocurriendo, por ejemplo:

- Alertas de sensores de un servidor.
- Una alerta del antivirus
- La caída de un servidor o sistema
- Accesos lentos

Signos precursores: son los que nos pueden indicar que un incidente tiene posibilidades de ocurrir en el futuro, por ejemplo:

- La detección de un escáner de puertos
- El resultado del análisis de vulnerabilidades
- Las amenazas de ataque por parte de hackers

DETECCIÓN Y ANÁLISIS

Es evidente que no se podrá gestionar un incidente si éste no se ha detectado.

CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de Ciberincidentes

35. Básicamente, los indicios de que nos encontramos ante un ciberincidente pueden provenir de dos tipos de fuentes: los *precursores* y los *indicadores*. Un **precursor** es un indicio de que *puede ocurrir* un incidente en el futuro. Un **indicador** es un indicio de que un incidente *puede haber ocurrido o puede estar ocurriendo ahora*.

- La caída
- Accesos

Signos precu
posibilidades de ocurrir en el futuro, por ejemplo:

- La detección de un escáner de puertos
- El resultado del análisis de vulnerabilidades
- Las amenazas de ataque por parte de hackers

IDENTIFICACIÓN DEL INCIDENTE

El primer paso consiste en identificar el tipo de incidente ocurrido y si ha ocurrido más de uno, priorizarlos dependiendo de su gravedad. Hay una guía del CCN, actualizada recientemente que trata este tema.

NOTIFICACIÓN DEL INCIDENTE

El proceso de notificación de incidentes de seguridad pasa por las siguientes acciones: reportar, notificar y registrar el incidente e iniciar el seguimiento en un evento de gestión. En función del tipo de incidente, éste se asignará y escalará a las personas que procedan para asegurar, en la medida de lo posible, su análisis, resolución y cierre.

CLASIFICACIÓN Y PRIORIZACIÓN DE INCIDENTES

Una vez detectado un incidente, hay que clasificarlo. Se pueden usar para la clasificación los siguientes factores:

CCN-STIC-817 Esquema Nacional de Seguridad. Gestión de Ciberincidentes

31. Los factores que podemos considerar a la hora de establecer criterios de clasificación son, entre otros:
    - **Tipo de amenaza:** código dañino, intrusiones, fraude, etc.
    - **Origen de la amenaza:** Interna o externa.
    - La **categoría**[3] de seguridad de los sistemas afectados.
    - El **perfil de los usuarios afectados**, su posición en la estructura organizativa de la entidad y, en su consecuencia, sus privilegios de acceso a información sensible o confidencial.
    - El **número y tipología de los sistemas afectados**.
    - El impacto que el incidente puede tener en la organización, desde los puntos de vista de la protección de la información, la prestación de los servicios, la conformidad legal y/o la imagen pública.
    - Los **requerimientos legales y regulatorios**.
32. La combinación de uno o varios de estos factores es determinante a la hora de tomar la decisión de crear un ciberincidente o determinar su peligrosidad y prioridad de actuación.

CLASIFICACIÓN Y PRIORIZACIÓN DE INCIDENTES

Y aunque la guía que se reeditó en Junio de 2018, incide en que para clasificar el incidente uno de los factores es

- El número y tipología de los sistemas afectados.

No hay una sola referencia a clasificar el incidente y relacionarlo con que se trate de una maquina con el paradigma IoT.

En cuanto a la Priorización es algo que en cada organización debemos establecer, pero creo que por el desconocimiento que tenemos aún de los incidentes relacionados con IoT, y según el tipo de equipos que se trate, sera “el sentido común” quien deba decirnos que prioridad asignamos a este tipo de incidentes.

CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

Las estrategias de contención de incidentes varían dependiendo del tipo de incidente, así como del posible impacto.

> En función de la gravedad de los incidentes, puede que sea necesario aplicar medidas como deshabilitar servicios, apagar sistemas o desconectarlos de la red, para intentar evitar que el incidente se extienda por la empresa.

Estas decisiones pueden facilitarse y agilizarse si se han definido previamente estrategias y procedimientos para contener los distintos tipos de incidentes posibles.

Una vez contenido el incidente, hay que verificar si es necesario eliminar o limpiar componentes asociados al incidente, además de proceder a la recuperación de todos los sistemas afectados, para devolverlos a la situación de operación normal.

CONTENCIÓN, RESOLUCIÓN Y RECUPERACIÓN

Posibles acciones para la resolución:

- Instalación de parches de seguridad
- Cambios en el cortafuegos
- Cambios en las listas de acceso

Posibles acciones de recuperación:

- Restaurar información desde las copias de seguridad Reemplazar componentes afectados con otros limpios de infección
- Instalar actualizaciones de software
- Cambiar contraseñas
- Reforzar la seguridad actualizando reglas de cortafuegos.

LECCIONES APRENDIDAS

En el plano del IoT, tendremos que ir sobre la marcha, pero necesitamos recopilar información sobre:

- Malas configuraciones de los dispositivos.
- Contraseñas inseguras.
- Trafico cifrado o no.
- Reacción del fabricante del equipo, (celeridad y calidad en la respuesta).
- Conexiones innecesarias.
- Protección de accesos al equipo.
- Repetición de incidentes sobre un mismo equipo.

CONCLUSIONES

- Profundizar en la legislación sobre dispositivos IoT
- Análisis de riesgos de estos dispositivos, al igual que lo hacemos sobre los que no son IoT
- Medidas de prevención tanto sobre los que ya tenemos como sobre los que vamos a adquirir.
- Gestionar la vulnerabilidades como las gestionamos sobre dispositivos que no son IOT
- Diferenciar en los incidentes si se trata de incidentes sobre dispositivos IoT.
- Incluir estos dispositivos en nuestro SGSI y en nuestro sistema de cumplimiento.
- Aplicar medidas de protección proporcionales al riesgo.

REFERENCIAS

- https://es.wikipedia.org/wiki/HL7
- https://www.bbvanexttechnologies.com/blog/nuevas-amenazas-en-google-home-quieres-saber-como-descubrimos-un-ataque-por-ecualizador/
- https://www.gartner.com/doc/3880164/evolving-iot-security-risks-demand
- https://www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691
- https://www.wired.com/2017/03/medical-devices-next-security-nightmare/
- https://www.ccn-cert.cni.es/ens.html
- https://youtu.be/k6ovFgIZ9nw (video del ataque man in the middle)
- https://www.helpnetsecurity.com/2018/10/05/iot-legislation-bans-shared-default-passwords/
- https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
- https://www.fda.gov/medicaldevices/digitalhealth/
- https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf
- https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
- https://www.congress.gov/bill/115th-congress/senate-bill/1691/all-info

XII Jornadas STIC CCN-CERT

Ciberseguridad, hacia una respuesta y disuasión efectivas

- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional