Infraestructuras Críticas

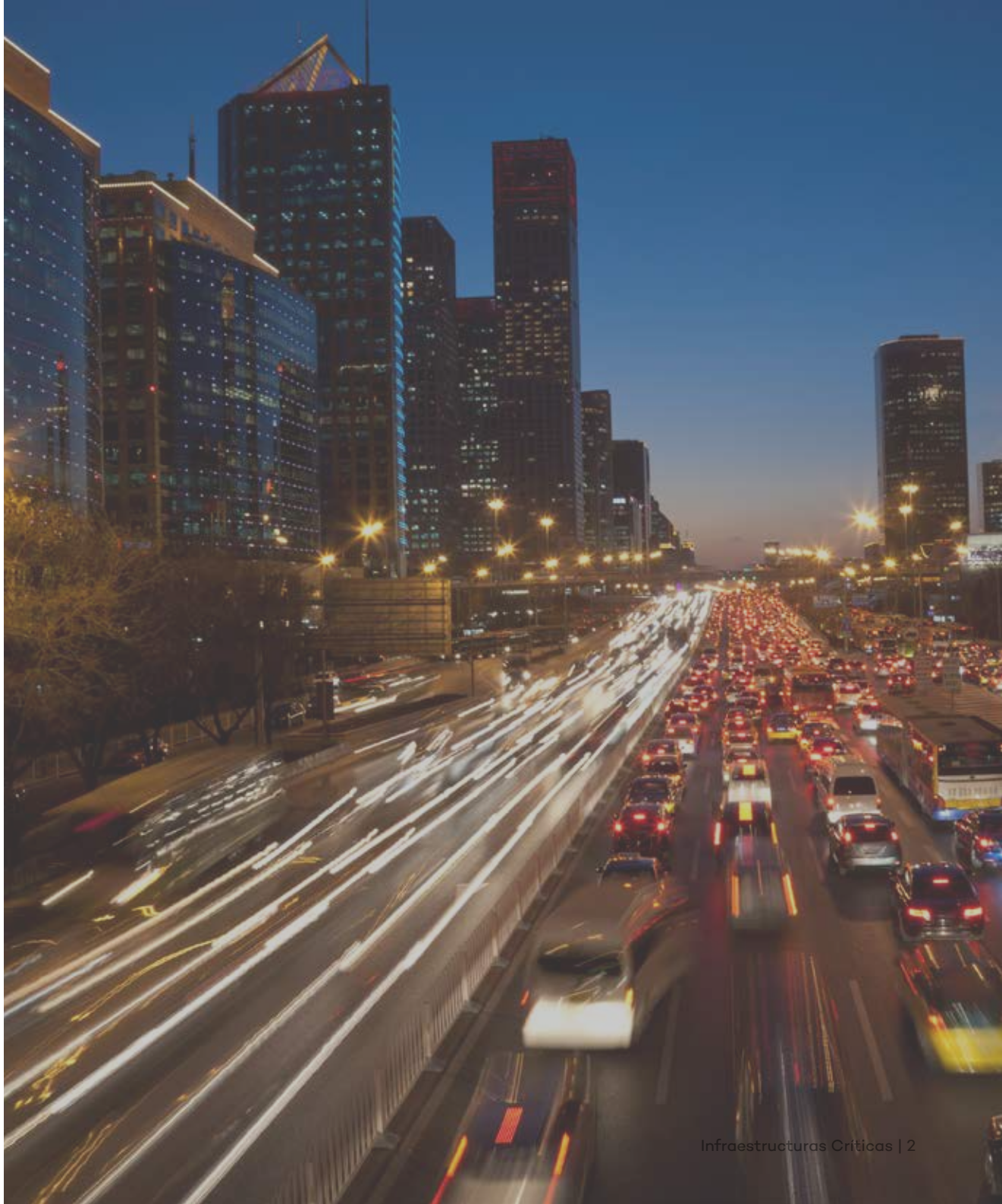
panda

Introducción

Hoy en día una de las fortalezas de las sociedades avanzadas es, al mismo tiempo, una debilidad. En un contexto hiperconectado como en el que vivimos, las sociedades desarrolladas y altamente tecnificadas dependen en extremo de una serie de servicios que se han convertido en esenciales.

Las infraestructuras son necesarias para el funcionamiento normal de los servicios básicos y los sistemas de producción de cualquier sociedad. De tal manera que cualquier interrupción, ya sea debida a causas naturales, técnicas, o por ataques deliberados, tendrían graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además se suponer un riesgo de seguridad.

Los delitos informáticos han experimentado una tendencia creciente a nivel mundial durante los últimos años. Una conectividad y un proceso de transformación digital que funciona como un arma de doble filo, ya que facilita y conlleva que los delincuentes pretendan cada vez más obtener resultados criminales. Pero, ¿qué pasa cuando son las redes que entendemos como necesarias para subsistir las que están en la diana del cibercrimen?



Sectores sensibles e infraestructuras críticas

La protección de las infraestructuras críticas es una preocupación de los Estados. El alto nivel de desarrollo de las sociedades actuales descansa en su mayor parte en una serie de servicios básicos y esenciales cuya prestación radica mayoritariamente en el sector privado.

Nunca las infraestructuras han sido tan trascendentales para el normal funcionamiento de los servicios y de los principales sistemas de producción como lo son la Administración, el agua, el sistema financiero y tributario, la energía, el espacio, la industria nuclear o el transporte, entre otros.

Aquellas instalaciones, redes, servicios y equipos cuya interrupción puede tener una repercusión importante en la salud, la seguridad o el bienestar económico de los ciudadanos, son las que entendemos como infraestructuras críticas.

Garantizar la seguridad de los suministros de estos servicios básicos ante nuevas amenazas es una responsabilidad no sólo de las administraciones públicas, sino también de los operadores privados a nivel nacional e internacional.

Características técnicas

Las particularidades técnicas y la alta exposición de los datos que pueden ser robados, hacen que la protección de este tipo de redes sea especial.

Estas nuevas intromisiones, dirigidas a los sistemas Ciberfísicos de los procesos industriales que se ejecutan en las infraestructuras críticas, hacen necesaria la adopción de nuevas estrategias capaces de detectarlos sin interferir en su funcionamiento normal.

Arquitectura híbrida

Para empezar, muchas de las infraestructuras catalogadas como críticas poseen una arquitectura híbrida en la que coexisten redes de tecnologías de información clásicas (Red IT) y redes de control industrial (Red OT) que gestionan los elementos que interactúan con el medio físico (Sistemas Ciberfísicos).

Aislados de Internet

Es importante prestar atención a este punto, puesto que, con la tendencia a interconectar cada vez más todo tipo de infraestructuras, se amplían también los posibles puntos de ataque. Si pensamos en cómo están organizados los sistemas de control de una de estas infraestructuras, normalmente se encuentran en su mayoría aislados de Internet y solo se comunican entre sí a través de una red interna.

SCADA

Sin embargo, también podemos encontrar ejemplos de sistemas de control SCADA que están visibles e incluso accesibles desde Internet. La mayoría de estos sistemas no tienen una relación directa con aquellos que se encargan de gestionar las infraestructuras críticas, pero sí que pueden ser una puerta de entrada para que un atacante obtenga información confidencial que le permita elaborar un ataque más sofisticado.

Tipología de ataques a Infraestructuras Críticas

Los estados modernos se enfrentan a multitud de desafíos que afectan a su seguridad nacional.

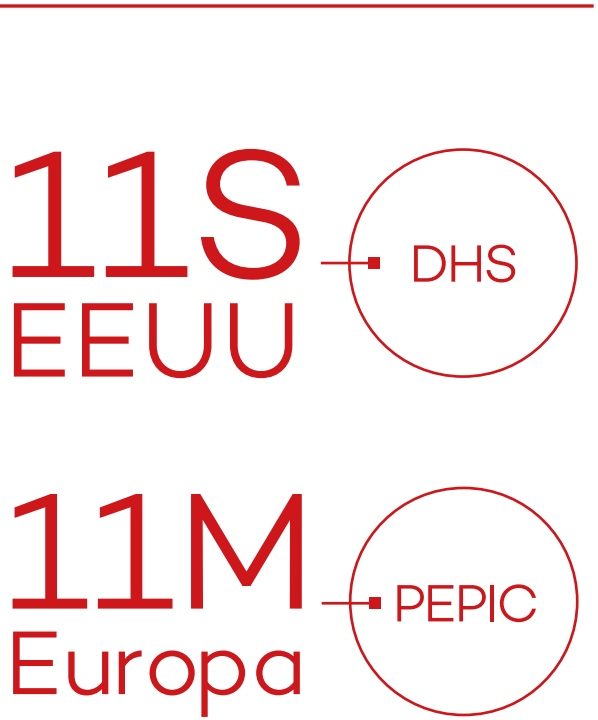
Dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, expuestas a una serie de amenazas. Para securizarlas es imprescindible catalogarlas y diseñar un plan de prevención y protección contra las posibles amenazas. Tanto en el plano de la seguridad física, como tecnológicas y las comunicaciones.

A lo largo de estos años ha habido acontecimientos clave que han marcado un antes y un después en el escenario de la seguridad mundial, como fue el 11 de septiembre de 2001. A partir de esta fecha se configuró un panorama en el que la destrucción de ciertos objetivos podría afectar a la vida, salud y bienestar tanto de los ciudadanos como de los Estados.

El tratamiento tradicional de la seguridad con relación a estos objetivos ha cambiado completamente. Hasta entonces, la seguridad era una competencia pública y exclusiva del Estado. Sin embargo, las infraestructuras críticas están en su mayoría en el sector privado, y este sector tiene también una responsabilidad en este ámbito. Tras el 11S, Estados Unidos reaccionó con la creación del Departamento de Seguridad Interior y una nueva y amplia regulación de esta materia.

A nivel europeo, la iniciativa surgió a raíz de otra fecha clave: el 11M. La Comisión Europea elaboró una estrategia global sobre protección de infraestructuras críticas, el “Programa europeo para la protección de infraestructuras críticas” que incluía propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas.

La Directiva establece, entre otras cosas, que la responsabilidad principal y última de proteger las infraestructuras críticas corresponde a los Estados miembros y a los operadores de las mismas, e insta a la implantación de una serie de iniciativas y actuaciones por parte de los Estados para su transposición a las legislaciones nacionales.



Un historial de ataques comprometidos

El gran público cree que aunque puede haber riesgo, apenas han existido ciberataques a infraestructuras críticas. Desafortunadamente la realidad es otra y existen cientos de casos documentados alrededor de todo el mundo.

Los ataques a estas redes coexisten con nosotros desde hace décadas, pudiendo elaborar un análisis cronológico de los más representativos.

Oleoducto siberiano

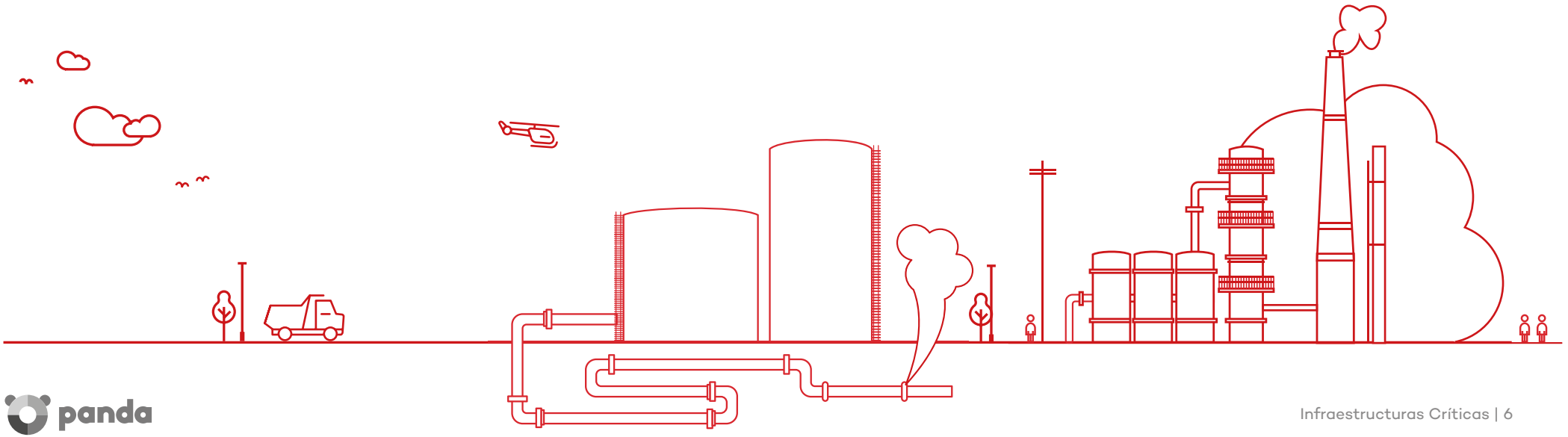
Al pensar en ciberataques a infraestructuras críticas, el término Internet nos vendrá a la mente de forma casi inmediata. Sin embargo el primer ciberataque de este estilo sucedió mucho antes de que Internet existiera. Tuvo lugar en **1982,** cuando los atacantes consiguieron instalar un troyano en el sistema SCADA que controlaba el oleoducto siberiano y que provocó una enorme explosión en el mismo. El ataque fue orquestado por la CIA, y no se supo de él hasta el año 2004, cuando Thomas C. Reed, antiguo subsecretario del Ministerio de Defensa de Estados Unidos y asesor de Ronald Reagan, publicó el libro "At the Abyss: An Insider's History of the Cold War", donde desvelaba esta historia.

Explosión en un oleoducto siberiano orquestado por la CIA

Chevron

El siguiente incidente tuvo lugar en **1992,** cuando un trabajador fue despedido de la compañía petrolera Chevron, hackeando los ordenadores de la compañía en Nueva York y San José que se encargaban del sistema de alertas y los reconfiguró para que dejaran de funcionar cuando se pusieran en marcha. No se descubrió el sabotaje hasta que en Richmond, California, hubo un incidente en el que se liberó una sustancia nociva y el sistema no mandó la alerta correspondiente, poniendo en riesgo a miles de personas durante las 10 horas en las que el sistema estuvo sin funcionar.

Liberación de una sustancia nociva que puso en riesgo a miles de personas



Salt River Project

En agosto de **1994** Lane Jarret Davies consiguió entrar a la red del Salt River Project a través de un módem, consiguiendo acceso a información y borrando ficheros de los sistemas responsables de la monitorización y entrega de agua y electricidad a sus consumidores. También consiguió acceso a información personal y financiera tanto de clientes como de trabajadores.

Aeropuerto Worcester

El sector aéreo también ha sufrido ataques dirigidos. El 10 de marzo de **1997** un hacker se coló en el sistema de control utilizado para las comunicaciones de tráfico aéreo en el aeropuerto de Worcester, Massachusets, causando un fallo que dejó inutilizado el sistema de telefonía durante 6 horas. En concreto afectó a los servicios telefónicos de la torre de control, el dpto. de bomberos del aeropuerto, el del servicio meteorológico y las compañías aéreas que estaban en el aeropuerto.

Gazprom

En **1999,** un hacker consiguió burlar los sistemas de seguridad de la rusa Gazprom –con ayuda de alguien que trabajaba en la empresa- y consiguió el control de los sistemas SCADA de la compañía, en concreto la centralita central encargada de manejar los flujos de gas. Para ello utilizó un troyano. Afortunadamente no tuvo mayores consecuencias y en cuestión de horas la empresa recuperó el control.

Borrado de los sistemas de entrega de agua y electricidad a los consumidores

Fallo en el sistema de telefonía de la torre de control, el dpto. de bomberos, el servicio meteorológico y las compañías aéreas durante 6 horas

Control de la centralita central encargada de manejar los flujos de gas

Maroochy Water System

Dos años de prisión fue la condena impuesta a un exempleado del Maroochy Water System que en el año **2000** hackeó con material robado a la empresa el sistema de control de aguas y provocó un vertido de un millón de litros de aguas residuales en un río cercano, inundando también los bajos de un hotel.

Planta de gas

Una planta de procesamiento de gas operada por una compañía petrolífera de EEUU sufrió un ataque en **2001.** Tras una investigación que duró 6 meses, se averiguó que fue obra de uno de sus proveedores, que de cara a encubrir un error que habían provocado en uno de los ordenadores crearon esta "distracción" hackeando 3 sistemas de la empresa y provocando el corte de gas en hogares y empresas de un país europeo.

PDVSA

En diciembre de **2002,** la petrolera venezolana PDVSA sufrió un ataque que bajó la producción de petróleo del país ese día de 3 millones de barriles a 370.000. El ataque se llevó a cabo hackeando diferentes ordenadores dentro de la compañía. Tuvo lugar mientras personal de la empresa estaba en huelga, por lo que todo apuntó a que se trató de un sabotaje realizado por uno de sus empleados.

Vertido de un millón de litros de aguas residuales en un río cercano

Corte de gas en hogares y empresas de un país europeo

Reducción de la producción de petróleo de 3 millones de barriles a 370.000

Semáforos de los Ángeles

En **2006,** dos ingenieros de tráfico de Los Ángeles hackearon los semáforos de la ciudad durante una protesta laboral. Cambiaron la programación de algunos de ellos – estratégicamente escogidos en cruces con mucho tráfico- para que la luz roja para vehículos estuviera mucho más tiempo activada, generando grandes atascos.

Tranvías de Lodz

En **2008**, un estudiante polaco de 14 años hackeó el sistema de tranvías de la ciudad de Lodz, en Polonia. El resultado: 4 tranvías descarrilaron, causando heridas a 12 personas. El estudiante construyó un mando infrarrojos similar a un mando de televisión con el que podía controlar los cruces de vías.

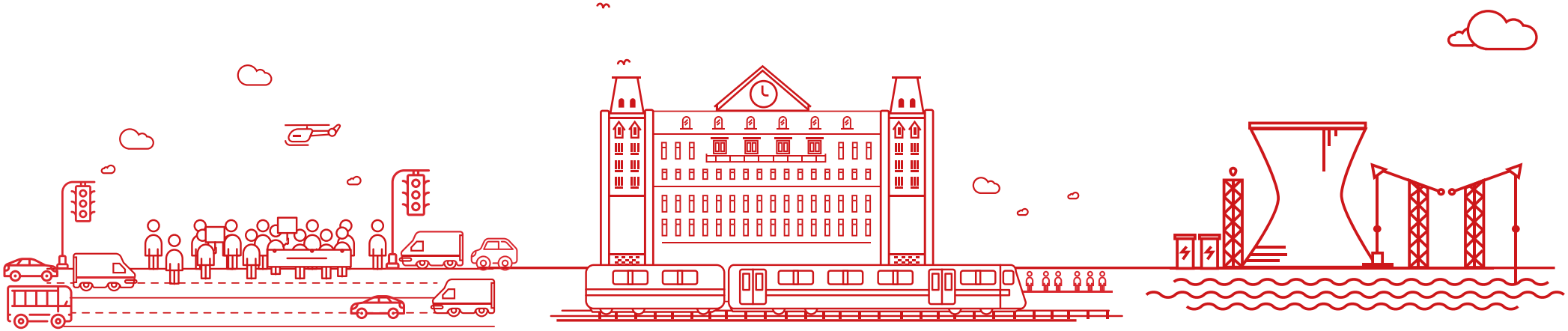
Saudi Aramco

En **2012,** la mayor compañía petrolera del mundo, Saudi Aramco, fue víctima de un ataque dirigido en su cuartel general. Los atacantes habían conseguido acceso a la red a través de un ataque a uno de sus empleados, y desde ahí consiguieron acceso a 30.000 ordenadores de la compañía. En un momento dado los atacantes borraron el contenido de todos los ordenadores al mismo tiempo que en la pantalla se mostraba una bandera estadounidense en llamas. Un grupo autodenominado “Cutting Sword of Justice” se hizo responsable del ataque.

Grandes atascos en zonas con mucho tráfico

4 tranvías descarrilados y 12 personas heridas

Ordenadores borrados con un salvapantallas de la bandera estadounidense en llamas



RasGas

Tan solo dos semanas después del ataque a Saudi Aramco, la empresa qatarí RasGas, la segunda mayor productora de gas natural licuado del mundo, sufrió un ataque con el mismo malware utilizado en la petrolera saudí. Durante varios días tanto la red interna de la empresa como su página web estuvieron inoperativas.

La red interna de la empresa y su página web estuvieron inoperativas

Planta metalúrgica alemana

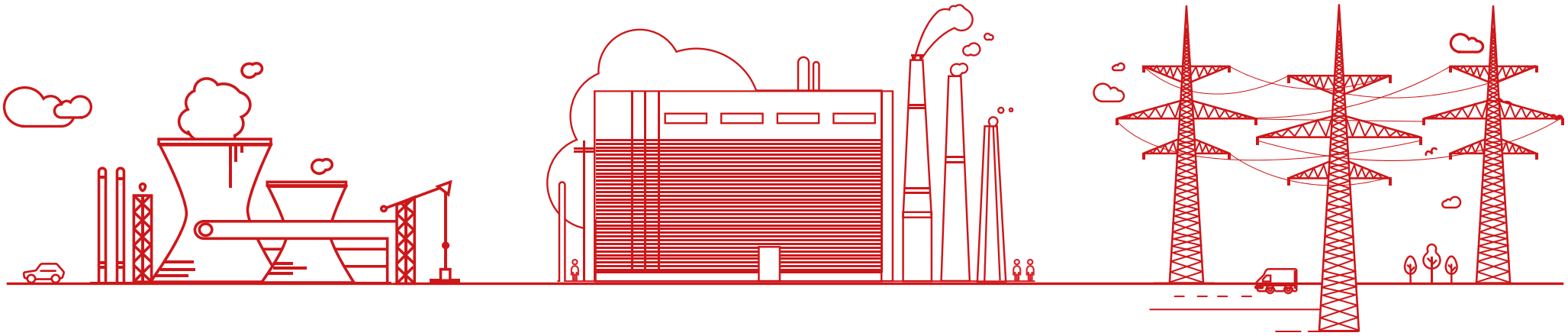
En **2014**, una planta metalúrgica de Alemania fue víctima de un ataque. A través de técnicas de ingeniería social los atacantes consiguieron acceder al ordenador de un empleado, y desde allí consiguieron acceso a la red interna del sistema de control. Como consecuencia de esto, al apagar uno de los altos hornos este no obedeció y se quedó encendido, lo que causó un daño masivo en las instalaciones.

Daño masivo en las instalaciones

Red eléctrica ucraniana

A finales de **2015**, Ucrania sufrió un ciberataque a su red eléctrica que dejó sin energía a más de 600.000 habitantes del país.

Más de 600.000 ucranianos sin energía



Primer ciberataque de la historia contra la infraestructura de Internet

A pesar de este largo historial, el primer ciberataque de la historia contra la infraestructura de Internet en un país no fue hasta el 27 de abril de **2007**. **Sucedió en Estonia, donde se sucedieron una serie de ataques que colapsaron las páginas web de multitud de organizaciones,** incluyendo la del parlamento, ministerios, bancos, periódicos y otros medios de comunicación, etc. Pero el ataque también fue contra direcciones de red no conocidas públicamente, entre las que se incluían el procesamiento de órdenes financieras y de servicios de telecomunicaciones del país.

Urmas Paet, ministro de Exteriores del gobierno estonio acusó públicamente al gobierno ruso de estar detrás de los ataques, aunque no pudo aportar pruebas que corroboraran su acusación.

El ciberataque a infraestructuras críticas más conocido de la historia: Stuxnet

En **2008** tuvo lugar el que sin duda ha sido el caso de ciberataque a infraestructuras críticas más conocido de la historia: **Stuxnet. A día de hoy se sabe que fue un ataque coordinado entre la inteligencia israelí y la norteamericana, con el objetivo de sabotear el programa nuclear iraní**.

Crearon un gusano que, al infectar los ordenadores que controlaban las centrifugadoras de uranio de la planta iraní de Natanz, hacía que éstas fueran a máxima velocidad mientras que al mismo tiempo la información mostrada en las pantallas de los terminales lo ocultaban, haciendo creer a los ingenieros que todo iba de forma normal.

Esto causó la rotura física de todas las centrifugadoras de uranio de la planta y el caso se convirtió en el mayor desencadenante que hizo tomar conciencia al gran público sobre este tipo de amenazas.

Los ataques comunes en el resto de empresas suceden también en estas instalaciones

Además de los ataques dirigidos específicamente a sabotear este tipo de infraestructuras, los mismos ataques que sufren el resto de empresas tienen lugar también en estas instalaciones y sus consecuencias, en ocasiones, han sido tan graves como las de los ataques dirigidos. **Este tipo de problemas comenzaron principalmente en los inicios de la década pasada, cuando comenzaron a popularizarse los gusanos de red que se propagan por sí mismos en cuanto llegan a una red**.

Un buen ejemplo fue lo sucedido en una importante fábrica de alimentación en EEUU tras una infección de virus que les costó miles de dólares. Uno de sus empleados se conectó de forma remota desde casa, y su ordenador estaba infectado con el virus Nimda por lo que, en cuanto entró en la red de la empresa, el gusano se propagó por todos los sistemas de control.

En 2003 una petrolera norteamericana se vio afectada por el gusano SQLSlammer cuando entró a la intranet de la empresa. No causó parada de la producción, pero sí afecto a las comunicaciones internas y llevó varios días poder eliminarlo completamente de la red y actualizar los sistemas para prevenir nuevos ataques. De hecho, este gusano ha sido uno de los que más estragos ha causado a empresas. Para propagarse utiliza una vulnerabilidad en servidores de bases de datos SQL (muy comunes en entornos corporativos). El parche de la vulnerabilidad fue publicado por Microsoft en enero de 2003, y otra compañía petrolera estadounidense comenzó a instalarlo en todas sus instalaciones en cuanto estuvo disponible, antes de que el gusano apareciera. Sin embargo, para acabar de instalarlo era necesario reiniciar los servidores donde se había aplicado, y varios de ellos estaban en plataformas petrolíferas que no contaban con trabajadores de IT, por lo que para supervisar la operación tenían que mandar personal especializado en helicóptero. Mientras estaban con este proceso el gusano apareció y los sistemas que no habían sido reiniciados fueron infectados.

El mismo 2003, uno de los mayores fabricantes de automóviles de EEUU sufrió el ataque del SQLSlammer, propagándose rápidamente y afectando a 17 de sus plantas de fabricación. El coste que tuvo para la compañía fue de 150 millones de dólares. A pesar de que el parche había estado disponible desde hacía 6 meses los responsables de IT de la compañía no lo habían aplicado.

El mismo año, una infección de malware (no se hizo público el malware causante del incidente) afectó a uno de los ordenadores de Air Canada que se encargaba de información de vuelo, carga de combustible, etc. Como consecuencia de esta infección 200 vuelos fueron retrasados y/o cancelados.

En Japón, en 2005, un empleado de Mitsubishi Electric resultó infectado con un malware, lo que provocó el filtrado de documentos de inspección confidenciales pertenecientes a 2 centrales nucleares pertenecientes a la compañía.

En un hospital de Reino Unido en 2006, dos ordenadores que se encargaban de manejar la aplicación del tratamiento de radioterapia en enfermos de cáncer resultaron infectados con malware. Tuvieron que retrasarse los tratamientos de 80 pacientes. Un par de años más tarde otros 3 hospitales del Reino Unido se infectaron con una variante del gusano Mytob lo que provocó que tuvieran que desconectar todos los ordenadores durante 24 horas para poder solucionar el incidente.

En 2013 ,una infección a 200 ordenadores del Cook County Department of Highway and Transportation, responsable del mantenimiento de cientos de kilómetros de autopistas en el área de Chicago. Como consecuencia del ataque tuvieron que desconectar la red durante 9 días para poder desinfectar todos los ordenadores.

Esta cronología pone en evidencia que el peligro de ciberataques al que las infraestructuras críticas están sometidas es real, y hoy en día todos los gobiernos son conscientes de los riesgos que implican.

Protección avanzada para infraestructuras esenciales

La realidad analizada y en la que vivimos hace necesario regular la Protección de las Infraestructuras Críticas para poder aportar un mayor grado de protección frente a amenazas de todo tipo.

En mayo de 2016, tras una reunión de ministros de Energía del G7, se hizo pública una declaración conjunta en la que, entre otros temas, se declaraba la importancia de lograr sistemas de energía resistentes -incluyendo la electricidad, el gas y el petróleo-, con el fin de responder eficazmente a las amenazas cibernéticas emergentes y mantener las funciones críticas.

Para mejorar la prevención y respuesta frente a ataques lógicos, los gobiernos están llevando a cabo distintas medidas a nivel global. Medidas orientadas a la creación de centros de coordinación que registren todo tipo de información relevante para aumentar la protección de las infraestructuras críticas. Como resultado, se ha desarrollado una estrategia global para atajar este problema, que debe incorporarse a las legislaciones nacionales.

Es difícil responder a la pregunta de si la seguridad en las Infraestructuras Críticas es la adecuada, ya que se desconoce la información o técnicas que pueden llegar a utilizar los ciberdelincuentes, por lo que nunca podemos estar seguros al 100%. Lo que sí se puede mejorar es la protección frente aquellos ataques conocidos y que pueden ser evitados adoptando una serie de buenas prácticas como las siguientes:

Buenas Prácticas

1. **Revisar los sistemas en busca de vulnerabilidades, especialmente aquellos que tengan agujeros de seguridad reportados y conocidos desde hace tiempo.**

2. **El control de medios extraíbles es esencial en una infraestructura, y no solo porque haya sido el vector de ataque usado en casos tan sonados como Stuxnet. A la hora de proteger una infraestructura crítica, tan crítico es evitar que un pendrive con código malicioso se cuele en la red interna como que se utilice ese mismo pendrive para sustraer información confidencial.**

3. **Las redes utilizadas para controlar estas infraestructuras deberían estar lo suficientemente vigiladas y, en aquellos casos que lo requieran, aisladas del exterior. De esta forma se podrían detectar ataques desde el exterior y se impediría que se accediese a sistemas controlados desde una red interna.**

4. **La supervisión del PC al que están conectados los controladores lógicos programables (o PLC). Son estos dispositivos conectados a Internet los más sensibles, ya que pueden proporcionar acceso a un atacante a ciertos sistemas de control sensibles. Además, aunque no consiga tomar el control de estos sistemas, podría obtener información valiosa para intentar otros vectores de ataque.**

La Solución

Una protección contra amenazas avanzadas y ataques dirigidos, e incluso, que sea capaz de detectar comportamientos extraños. Un sistema que pueda asegurar la confidencialidad de los datos, la privacidad de la información, el patrimonio y reputación empresarial.

Una plataforma inteligente que ayude al personal de seguridad de las redes críticas a reaccionar de forma más rápida ante las amenazas y garantizar que puedan disponer de la información correcta necesaria para responder de forma adecuada.

Esto es Adaptive Defense 360, el único sistema de ciberseguridad avanzado que combina protección de última generación y la última tecnología de detección y remediación con la capacidad de clasificar el 100% de los procesos en ejecución.

Adaptive Defense 360 clasifica absolutamente todos los procesos activos en todos los endpoint, garantizando la protección contra el malware conocido y contra amenazas avanzadas del tipo Zero-Day, Advanced Persistent Threats y Ataques Dirigidos.

La plataforma utiliza la lógica contextual para revelar patrones de comportamiento malicioso y generar acciones de ciberdefensa avanzada contra amenazas conocidas y desconocidas.

Analiza, categoriza y correlaciona todos los datos que obtiene sobre las ciberamenazas, para llevar a cabo tareas de Prevención, Detección, Respuesta y Remediación.

Averigua quién y cómo accede a tus datos y controla la fuga de información, la que intente realizar un malware o la que realicen tus empleados.

Descubre y soluciona las vulnerabilidades de los sistemas y de los programas instalados y previene la utilización de los no deseables (barras de navegación, adwares, add-ons,...).

Contacta con nosotros para más información

ARGENTINA
+54 11 6632 6632
argentina@pandasecurity.com

BOLIVIA
+59 12 21 20 300
bolivia@pandasecurity.com

BRASIL
+55 11 3054-1722
brazil@pandasecurity.com

CHILE
+56 2 6394774
chile@pandasecurity.com

COLOMBIA
+57 1 2560344
colombia@pandasecurity.com

COSTA RICA
+506 2523-4300
ventas@cr.pandasecurity.com

ECUADOR
+593 02 6012384
ecuador@pandasecurity.com

EL SALVADOR
+503 22087435
ventas.elsalvador@pandasecurity.com

GUATEMALA
+502 66400100
ventas.guatemala@pandasecurity.com

MÉXICO
+52 55 8000 2381
mexico@pandasecurity.com

PANAMÁ
+507 833 7263
ventas.panama@pandasecurity.com

PARAGUAY
+595 21 6075 94
paraguay@pandasecurity.com

PERÚ
+51 1 204 55 00
peru@pandasecurity.com

URUGUAY
+598 2 402 0673
ventas@uy.pandasecurity.com

VENEZUELA
+58 212-7612535
venezuela@pandasecurity.com

Más información:

pandasecurity.com/enterprise/solutions/adaptive-defense-360

Contacta:

900 90 70 80

panda

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

pandasecurity.com

panda