Seguridad Cibernética en la Cadena de Suministros.

Jaime Scarpatti

Consejero de Informatica

Embassy of the United States of America, Panama.

Leonel "Leo" Ruiz

Consejero de Seguridad Informatica

Embassy of the United States of America, Panama.

Seguridad Cibernética en la Cadena de Suministros.

- Se refiere al subconjunto de la seguridad de la cadena de suministro y se centra en la gestión de los requisitos de seguridad cibernética para los sistemas, las aplicaciones y las redes de tecnología de la información, que están impulsados por amenazas como el ciberterrorismo, el malware, el robo de datos y la amenaza persistente avanzada (APA).

Motivos Principales

Generalmente son dos los principales motivos para atacar una cadena de suministros:

- Economicos

- Interrupción de servicios.

Amenazas a la cadena de suministro

- 80% de ataques se dan en la cadena de suministros (KPMG).
- 56% de organizaciones han sufrido un ataque debido a un proveedor. (CSOOnline.com)
- Solo el 35% de las compañías tenía una lista de todos los terceros con los que compartían información confidencial.
- Solo el 18 por ciento de las empresas dice que sabía si esos proveedores, a su vez, compartían esa información con otros proveedores.

Ejemplos de ataques a la cadena de suministros

- Equipo y/o programas maliciosos (malware) instalados de fabrica.
  - Lenovo (Superfish-Visual Discovery)
  - SuperMicro (Producto alterado durante ensamblaje en China)

- Programas maliciosos (malware) instalados por malos actores (hackers).
  - Adobe Acrobat (Instalación de programa de mineria en aplicaciones validas)
  - SanDisk (Caballo de Troya en auto actualización)

- Vulnerabilidades existentes en programas (software) y equipos (hardware) dentro de la cadena de suministros que pueden ser encontrados por malos actores.
  - Target (ataque por medio de terceros)
  - Huawei (Cyber-security higiene)
  - OpenSSL (BleadingHart attack)

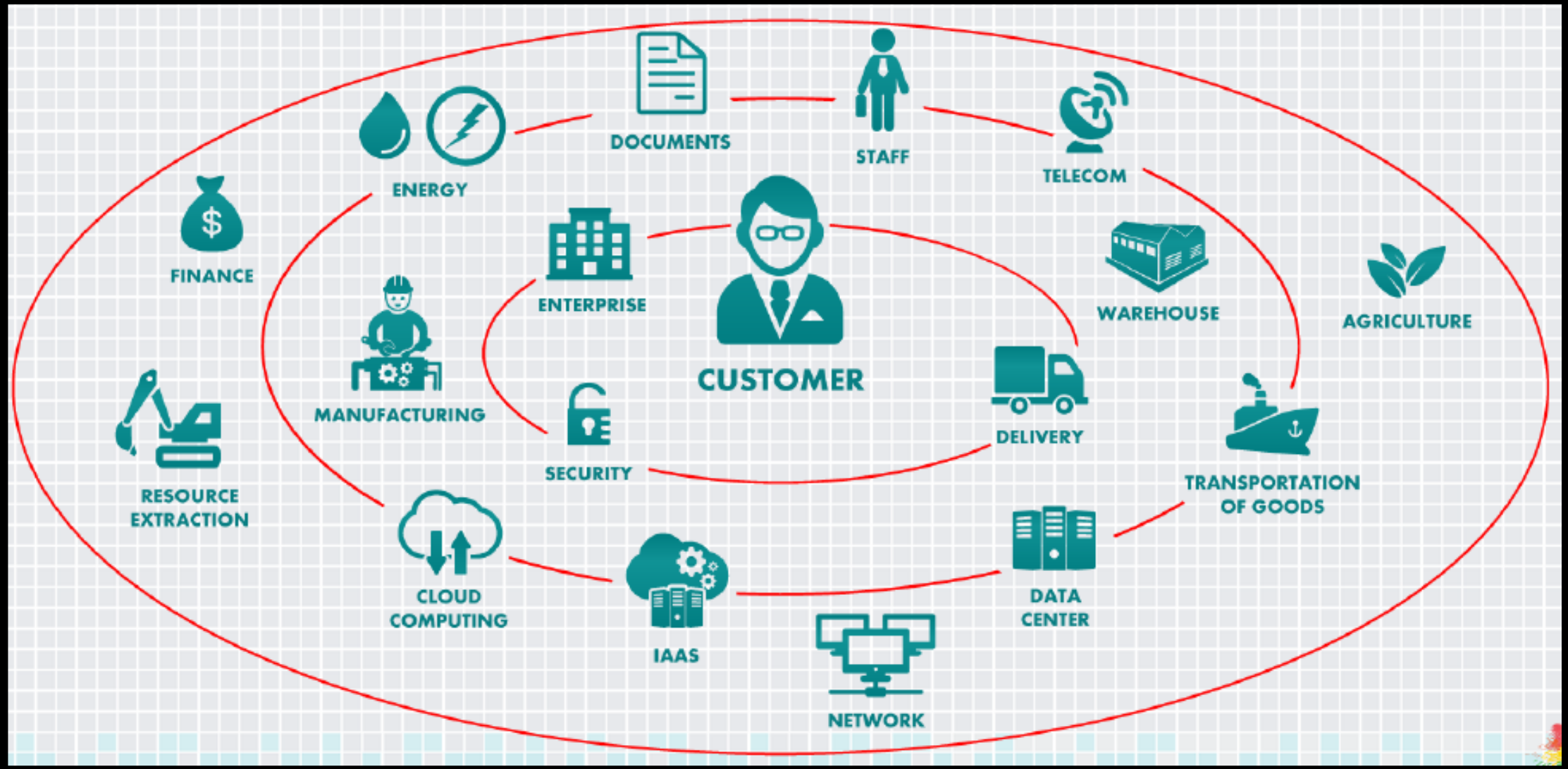
- Equipos y aplicaciones falsificados.
  - Microsoft, Adobe, Kingstone, Transcend

Responsabilidad de estándares de informática en Los Estados Unidos

nist.gov

NIST y los riesgos de la cadena de suministro cibernética.

Que consideran ustedes ser parte de la cadena de suministros?



Quienes ustedes consideran están a mas riesgo de ciberseguridad en la cadena de suministros?

Aclaramientos en la ciberseguridad en la cadena de suministros

- No se puede ver como un problema de IT solamente.

- Los riesgos de la cadena de suministro cibernética afectan la contratación, la gestión de proveedores, la continuidad y la calidad de la cadena de suministro, la seguridad del transporte y muchas otras funciones en toda la empresa y requieren un esfuerzo coordinado para abordarlas.

Principios de seguridad de la cadena de suministro cibernética:

- 1. Desarrolle sus defensas basándose en el principio de que sus sistemas serán violados.
- 2. La seguridad cibernética nunca es solo un problema de tecnología, es un problema de personas, procesos y conocimientos.
- 3. La seguridad es seguridad. No debe haber brecha entre lo físico y la ciberseguridad.

Riesgos clave de la cadena de suministro cibernética:

- Proveedores o proveedores de servicios de terceros, desde servicios de limpieza hasta ingeniería de software, con acceso físico o virtual a sistemas de información, código de software o IP.
- Prácticas deficientes de seguridad de la información por parte de proveedores de nivel inferior.
- Software o hardware comprometido comprado a los proveedores.
- Vulnerabilidades de seguridad del software en la gestión de la cadena de suministro o sistemas de proveedores.
- Falsificación de hardware o hardware con malware incrustado.
- Almacenamiento de datos de terceros o agregadores de datos

Ejemplos de las mejores prácticas de la cadena de suministro cibernética:

- Los requisitos de seguridad están incluidos en cada RFP y contrato.
- Las políticas de "una falla y estás afuera" con respecto a los productos de proveedores que son falsificados o que no coinciden con las especificaciones.
- Las compras de componentes están estrictamente controladas; las compras de componentes a proveedores aprobados están precalificadas. Las piezas compradas a otros proveedores se desempaquetan, se inspeccionan y se toman radiografías antes de ser aceptadas.
- Se establecen programas de desarrollo de ciclo de vida de software y capacitación para todos los ingenieros en el ciclo de vida.
- Se obtiene código para todo el software comprado.
- El software y el hardware tienen un apretón de manos de seguridad. Los procesos de arranque seguro buscan códigos de autenticación y el sistema no se iniciará si no se reconocen los códigos.
- La automatización de los regímenes de fabricación y prueba reduce el riesgo de intervención humana.

Que realmente estamos tratando de proteger?

- Información: datos
  - Confidencialidad
  - Integridad
  - Disponibilidad

Recientemente en el sector medico

If hackers can hide tumors in scans, what else can they hide?

The object on the doctor's screen, a white mass on a dark void, sits in the lungs, in a place it shouldn't be, and suggests cancer. The data that produced the image is saved and processed through a computer the physician knows about and one that remains entirely unknown to the hospital staff. But in a demonstration staged with the permission of an anonymous hospital, a team of security researchers have fooled the experts: the cancer on the screen is a mirage of code. Data integrity is every bit as important as anything else in cybersecurity. A study

Data breach may have exposed the personal, medical information of 600,000 in Michigan

The personal information and medical data of more than 600,000 people in Michigan may have been compromised in a cyberattack, the state's attorney general said Monday. Hackers may have accessed the names, addresses, social security numbers and medical information of customers of several Michigan healthcare companies, including Blue Cross Blue Shield of Michigan, Health Alliance Plan and McLaren Health Care, Dana Nessel said. The business that hackers targeted, Wolverine Solutions Group (WSG), a healthcare company that partners with health plans and hospital systems, said that it has begun notifying clients

Recientemente en el sector gubernamental

Russia internet freedom: Thousands protest against cyber-security bill

A mass rally in Moscow and similar demonstrations in two other cities were called after parliament backed the controversial bill last month. The government says the bill, which allows it to isolate Russia's internet service from the rest of the world, will improve cyber-security. But campaigners say it is an attempt to increase censorship and stifle dissent. Activists say more than 15,000 people gathered in Moscow on Sunday, which is double the estimate given by the police. Some protesters chanted slogans such as "hands off the internet" and "no to isolation" while others gave speeches on a large stage. Opposition figures said that a number of protesters were detained in Moscow, but the police have not confirmed this. The government says the so-called digital sovereignty bill will reduce Russia's reliance on internet servers in the United States. It seeks to stop the country's internet traffic being routed through foreign servers. A second vote is expected later this month. If it is passed it will eventually need to be signed by President Vladimir Putin.

https://www.bbc.com/news/world-europe-47517263

Recientemente en el sector de comercio

Email Marketing Firm Shuts Down After Exposing 800M Records

An email marketing firm accidentally exposed 800 million records, including people's phone numbers, dates of birth, and ZIP codes. The 150GB database was storing all the information online—in plain text with no password protection, according to the security researchers Bob Diachenko and Vinny Troia. Last month, Diachenko stumbled on the database, and discovered it contained a massive trove of 763 million email addresses. Each record was also structured to "include zip / phone / address / gender / email / user IP / DOB," Diachenko wrote in a Thursday blog post. "Although not all records contained the detailed profile information about the email owner, a large amount of records were very detailed," he said. "We are still talking about millions of records." Many of the records also contain other details such as Facebook, LinkedIn, and Instagram accounts linked to each email address, in addition to people's credit scores and personal mortgage amounts. So who created the database? Diachenko traced it back to a mysterious company called Verifications.io, which specializes in helping companies validate customer email records to keep them up to date. It explains why the database held so many records. "Unfortunately, it appears that once emails were uploaded for verification they were also stored in plain text," Diachenko said. "Once I reported my discovery to Verifications.io, the site was taken offline and is currently down at the time of this publication."

https://www.pcmag.com/news/367052/email-marketing-firm-shuts-down-after-exposing-800m-records

Que podemos hacer como clientes y usuarios?

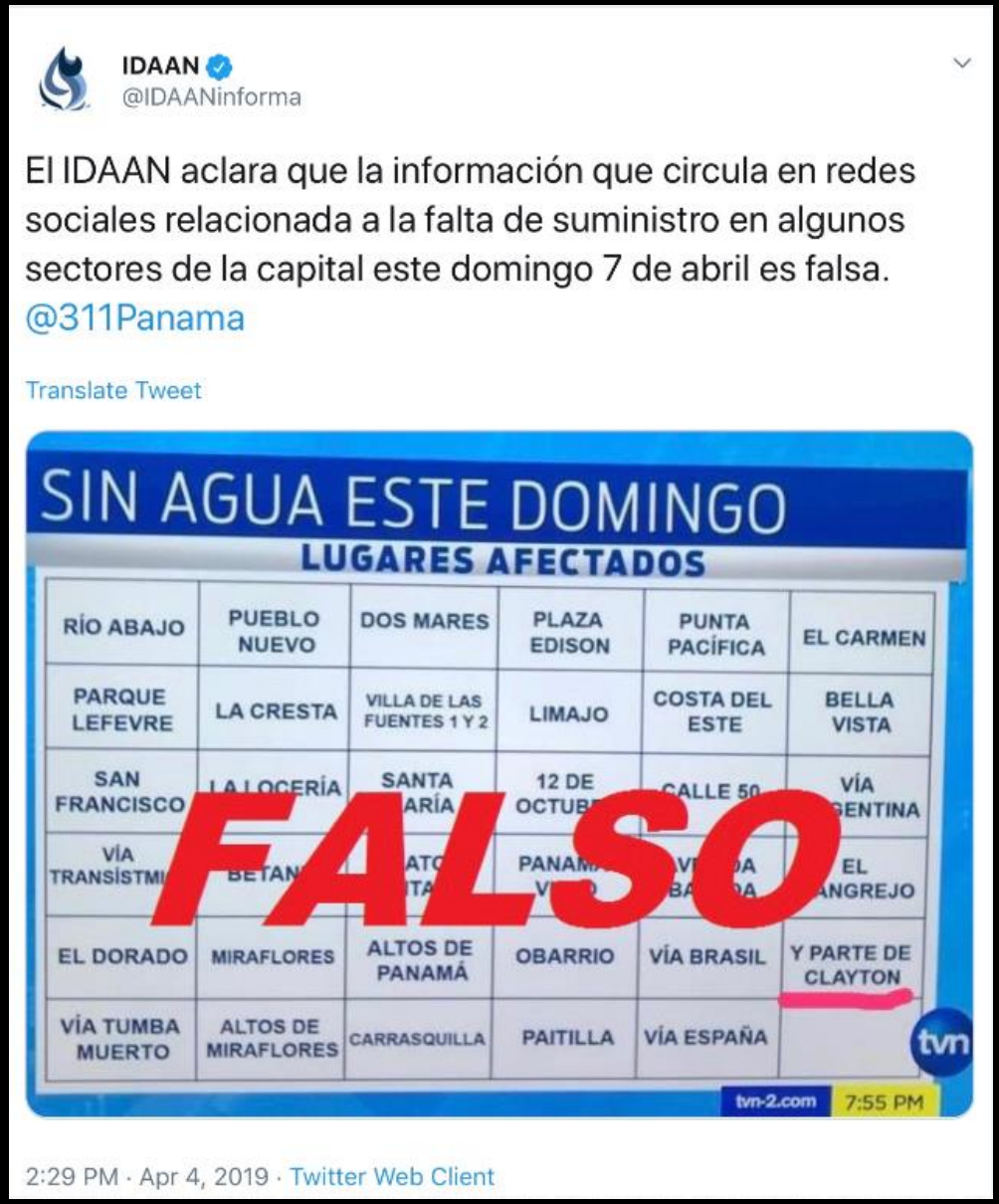
- Educación – Yo NO!
- Todo empieza en la seguridad de la casa – familia, IoT
- Vulnerabilidad en redes abiertas
- Vulnerabilidad en redes sociales
- Gratis no es mejor
  - Si no pago por el servicio, yo soy el producto

Que podemos hacer como empresarios?

- Educación – programa de ciberseguridad
- Ciber necesita un asiento en la mesa directiva
- Adquisición de servicios – software y hardware
- Seguridad en los servicios de nube – pago y gratis
- Monitoreo y mas monitoreo

Consecuencias del mal uso de información

- Reputación personal
- Reputación de negocios
- Importancia de chequeo y acceso de información en las cadenas sociales



Todas las plataformas son vulnerables …

Easter Attack Affects Half a Billion Apple iOS Users via Chrome Bug

About a half a billion Apple iOS users (and counting) have been hit by session-hijacking cybercriminals bent on serving up malware. They're exploiting an unpatched flaw in the Chrome for iOS browser, to bypass sandboxing and hijack user sessions, targeting iPhone and iPad users. The attacks are the work of the eGobbler

Facebook now says its password leak affected 'millions' of Instagram users

Facebook has confirmed its password-related security incident last month now affects "millions" of Instagram users, not "tens of thousands" as first thought. The social media giant confirmed the new information in its updated blog post, first published on March 21. "We discovered additional logs of Instagram passwords being

Millions of Medical Documents for Addiction and Recovery Patients Leaked

As if wrestling with addiction and recovery weren't difficult enough, tens of thousands of patients of a rehab clinic in Pennsylvania may find their personal information hijacked and manipulated by identity thieves or extortionists. An ElasticSearch database that was left open to the internet exposed about 4.9 million data points

Las leyes y el internet de las cosas. Quien nos protegerá?

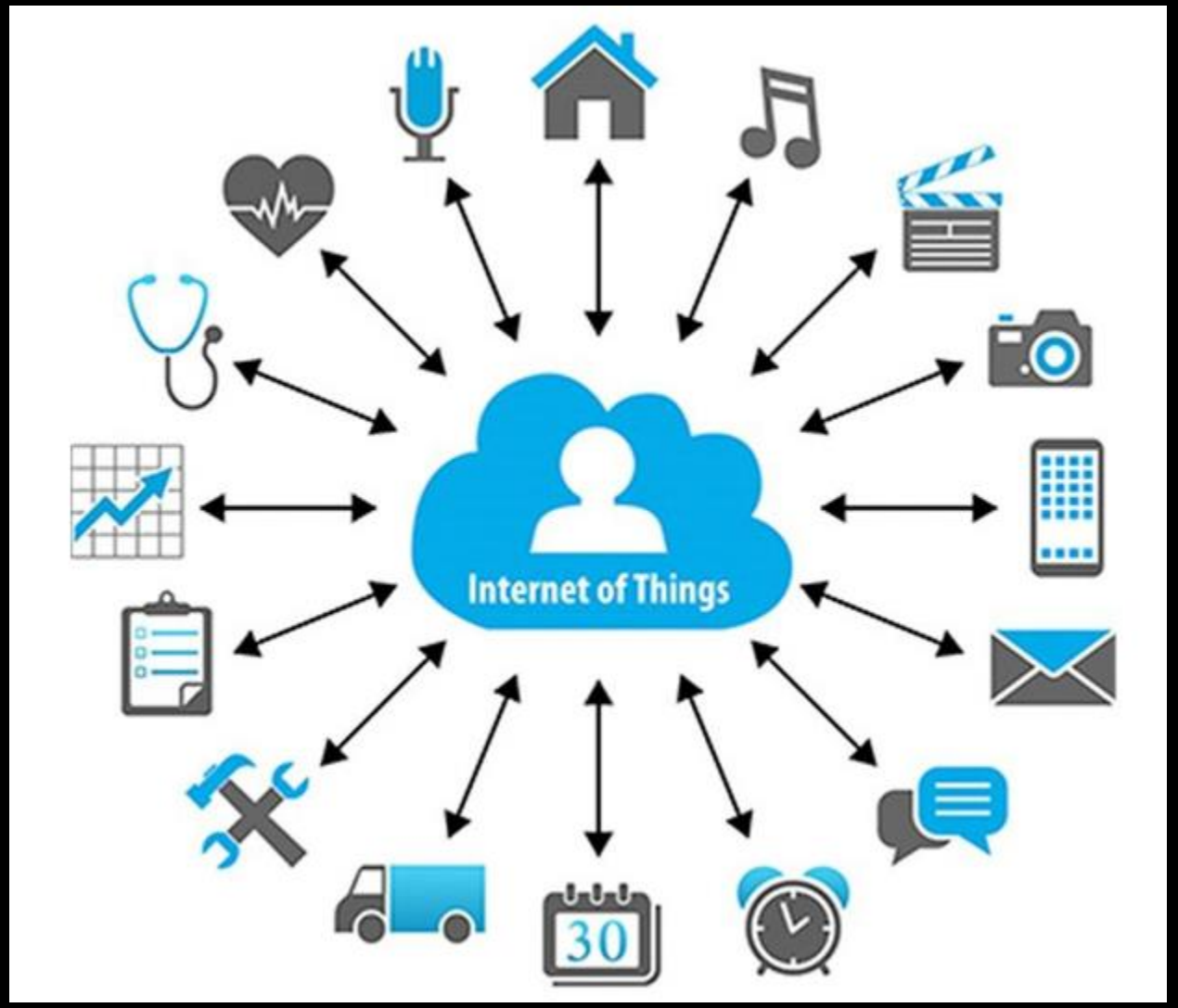
Can new laws protect you from smart home security breaches?

Jennifer Williamson
@Jennifer_for_OR

From Internet connected watches to Internet connected thermostats, as the Internet of Things is integrated into our most private areas, consumers should have the assurance that these devices are secure and fend off unwanted intrusion. #orpol #orleg

> **Mike Rogoway** @rogoway
> The Oregon House voted 53-5 today in favor of a bill requiring security for IoT devices.bit.ly/2DjARuy

♡ 23 6:41 PM - Apr 16, 2019



En Panama esta vigente la Ley 81 - GDPR

Ley No. 81 - Objetivo

Art. 1: Esta Ley tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos, por parte de las personas naturales o jurídicas, de derecho público o privado, lucrativas o no, que traten datos personales en los términos previstos en esta Ley. Toda persona, natural o jurídica, de derecho público o privado, lucrativo o no, puede efectuar el tratamiento de datos personales, siempre que lo haga con arreglo a la presente Ley y para los fines permitidos en el ordenamiento jurídico. En todo caso, deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos y de las facultades que esta Ley les reconoce.

La red de 5G y la revolución del manejo de datos en la cadena de suministro

- Cable & Wireless
- Digicel
- Movistar
- Claro

GSMA

Mobile360 Security for 5G — The Hague 28-29 May 2019

HEADLINE SPONSOR

HUAWEI

INDUSTRY SPONSORS

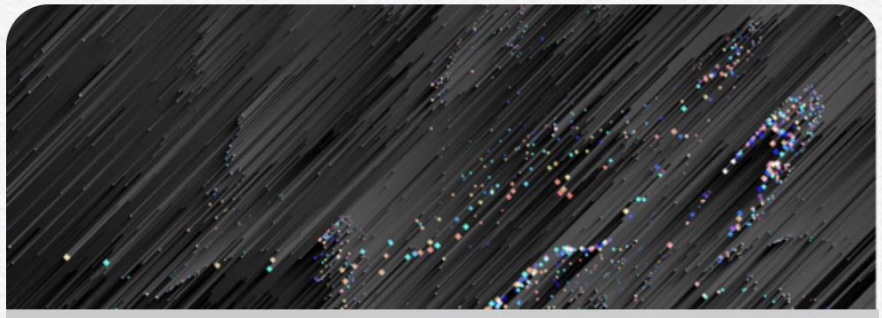
NetNumber syniverse ZTE

GLOBAL PARTNER

MOBILE WORLD CAPITAL BARCELONA

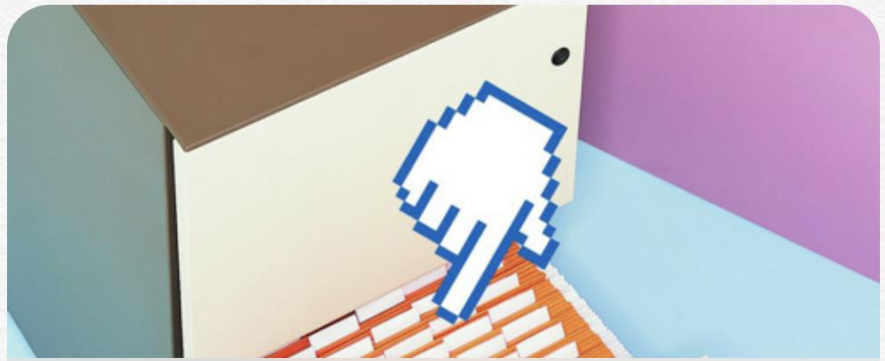
Ejemplos

How Nest, designed to keep intruders out of people's homes, effectively allowed hackers to
Tech companies are deciding between user convenience and potential damage to their brands.



Cyberattacks are rising sharply, but businesses are less prepared – and the cost is getting eye-
An exhaustive report of the state of cybersecurity among businesses has found that the number of companies reporting cyberattacks grew

Online passwords: Research confirms millions of people are using 123456 - Digital Trends
According to recent analysis of data caught up in cyber attacks, millions of people are continuing to use super-simple passwords, with 123456



Security Roundup: Facebook 'Unintentionally' Collected Email Contacts of 1.5 Million Users -
The Mueller report, Facebook goofs, and more of the week's top security news.

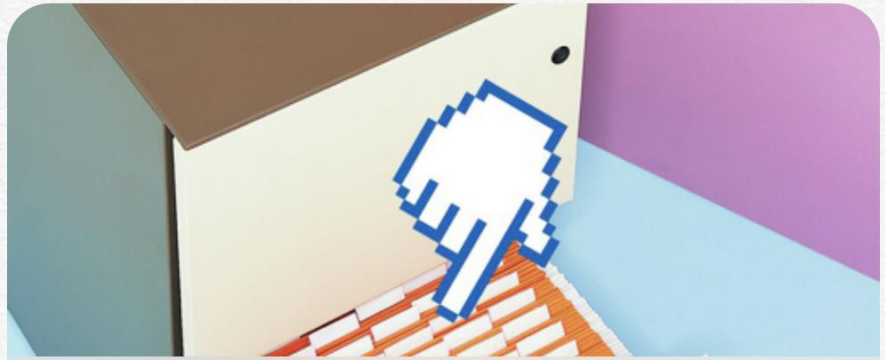
Ejemplos

Lawmakers are hoping to protect customers from smart home security breaches - Digital

To help combat smart home data breaches, state and federal lawmakers are exploring ways to protect consumers. California, Oregon, and

Supply Chain Hackers Snuck Malware Into Videogames - WIRED

An aggressive group of supply chain hackers strikes again, this time further upstream.



Security Roundup: Facebook 'Unintentionally' Collected Email Contacts of 1.5 Million Users -

The Mueller report, Facebook goofs, and more of the week's top security news.

You're being attacked like a nation state: Why aren't you defending like one? - The Hill

Nation states and private sector organizations are now being attacked by the same actors in much the same ways.

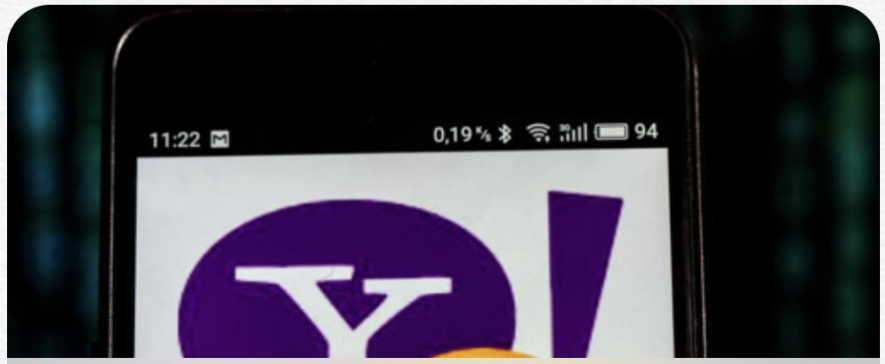
Ejemplos

Huawei says its equipment as secure as any, pans U.S. campaign - Reuters

China's Huawei Technologies said on Thursday the security of its telecoms network equipment was as tight as any, and hit back at the U.S.

The CIA says that China's security agencies provided funds for Huawei: report - The Verge

The US intelligence agency reportedly warned allies of links to China's government



Yahoo tries to settle 3-billion-account data breach with $118 million payout - Ars Technica

Verizon-owned Yahoo boosted offer after judge rejected first settlement.

China Using OPM Records for Spying - Washington Free Beacon

China is mining intelligence from an estimated 23 million records of American federal workers, including intelligence and security personnel,

Ejemplos

Well-funded surveillance operation infected both iOS and Android devices - Ars Technica
Malware that stole contacts, audio, location and more was under development for years.

Mysterious safety-tampering malware infects a second critical infrastructure site - Ars Technica
Use of game-changing Triton malware to target safety systems isn't an isolated incident.

Huawei's security troubles are hardening into a fight between the US and China - The Verge
The focus isn't on the company, but the legal system that governs it

Facebook says has made headway against abuses ahead of India election - Business
By Joseph Menn MENLO PARK, California (Reuters) - Facebook has said it has made strides in its efforts to prevent online abuses in the

Ejemplos

We aren't prepared for the next wave of cybersecurity risks - The Hill

Our government must lead the way.

Britain just laid out plans to end the internet's Wild West days and take a world-leading role in

UK prime minister Theresa May. Britain wants to end the internet's days as the Wild West by taking a world-leading role in regulating the

MIT halts collaborations with Chinese tech firms Huawei, ZTE - Reuters

The Massachusetts Institute of Technology (MIT) said on Wednesday it has halted collaborations with Huawei Technologies and ZTE Corp over

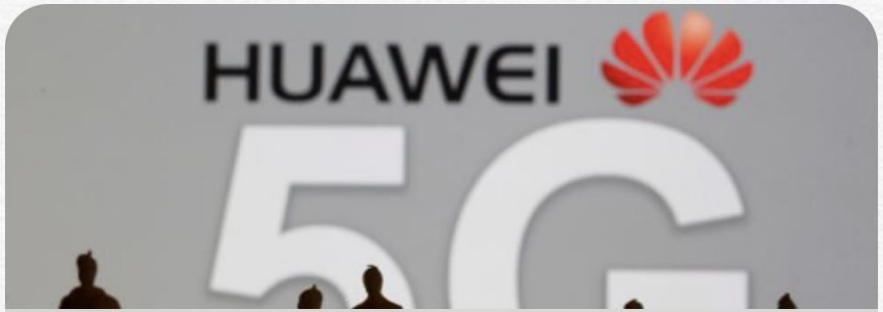
Former top US generals issue 'grave' warning to ban Chinese tech - CNN

Six retired US military leaders have issued a statement calling on America's allies to ban Chinese technology giants from outfitting their

Ejemplos

Asus software updates were used to spread malware, security group says - The Verge
The attack is named "ShadowHammer."

Bayer says has detected, contained cyber attack - Reuters
Germany's largest drugmaker, Bayer, said it had detected and contained a cyber attack on its computer networks, highlighting the risk of data



British security agency slams Huawei with 'scathing' report: Will it matter? - AEI
Last week, British cybersecurity officials issued a report "sharply critical" of Huawei, the Chinese telecoms giant that is the world's largest provider

U.S. Trade Negotiators Take Aim at China's Cybersecurity Law - The Wall Street Journal
U.S. and Chinese trade negotiators haggled over how to get Beijing to walk back China's tough cybersecurity law as both sides push to settle a

Additional resources.

- https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/nist_ict-scrm_fact-sheet.pdf
- https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
- https://www.darkreading.com/risk-management/homeland-security-devices-components-coming-in-with-malware/d/d-id/1098840
- https://howlingpixel.com/i-en/Supply_chain_cyber_security