X CONGRÉS ISACA BARCELONA 2021

UNA DÈCADA DE REPTES. UNA NOVA ÈPOCA PER L'AUDITORIA, SEGURETAT I PRIVACITAT

ISACA
Barcelona Chapter

X CONGRÉS
ISACA BARCELONA
2021

UNA DÈCADA DE REPTES.
UNA NOVA ÈPOCA PER
L'AUDITORIA, SEGURETAT
I PRIVACITAT

El eslabón más débil de la cadena ... de suministros

Fernando Cócaro, CISM

Ingeniero en computación (UdelaR - Uruguay), con más de 15 años de experiencia en el campo de la seguridad. Actualmente Global Cybersecurity Architect, ha desarrollado funciones de CSO, CISO, gerente del CERT nacional de Uruguay, entre otras.

ISACA
Barcelona Chapter

TECHNOLOGY NEWS DECEMBER 13, 2020 / 7:51 PM / UPDATED 10 MONTHS AGO

Suspected Russian hackers spied on U.S. Treasury emails - sources

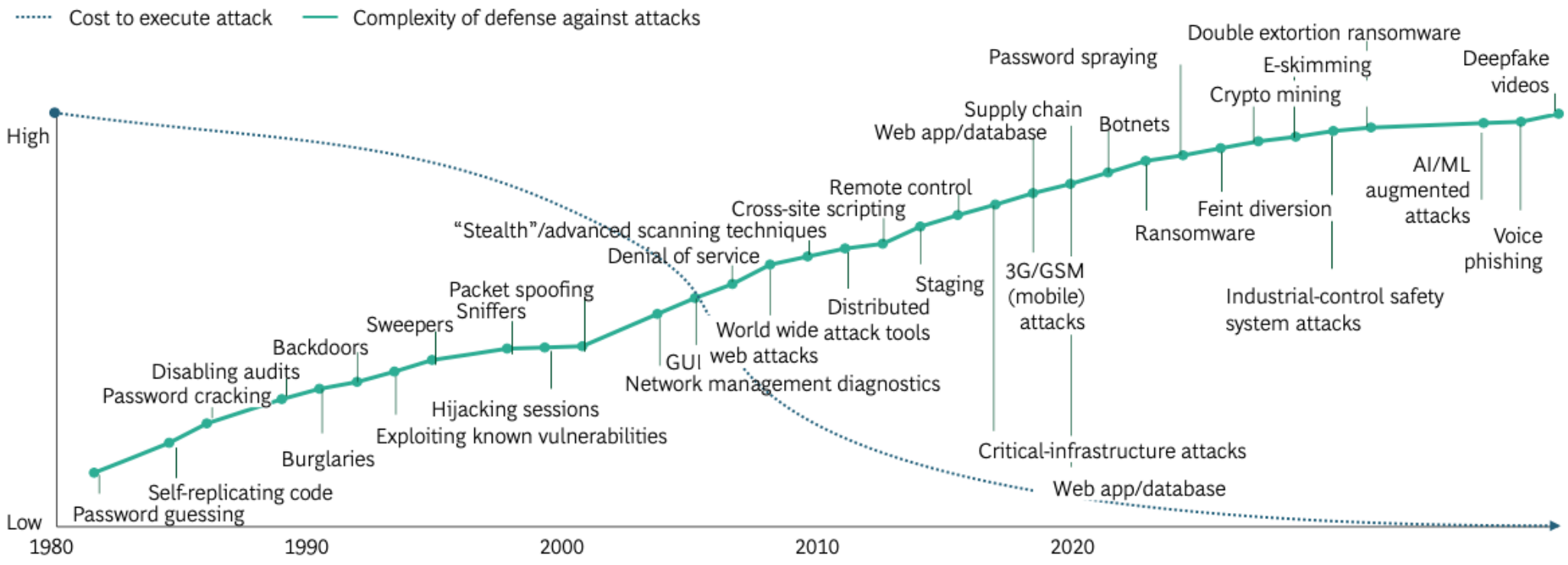
By Christopher Bing

5 MIN READ

WASHINGTON (Reuters) - Hackers believed to be working for Russia have been monitoring internal email traffic at the U.S. Treasury and Commerce departments, according to people familiar with the matter, adding they feared the hacks uncovered so far may be the tip of the iceberg.

The cyber spies are believed to have gotten in by surreptitiously tampering with updates released by IT company SolarWinds, which serves government customers across the executive branch, the military, and the intelligence services, according to two people familiar with the matter. The trick - often referred to as a "supply chain attack" - works by hiding malicious code in the body of legitimate software updates provided to targets by third parties.

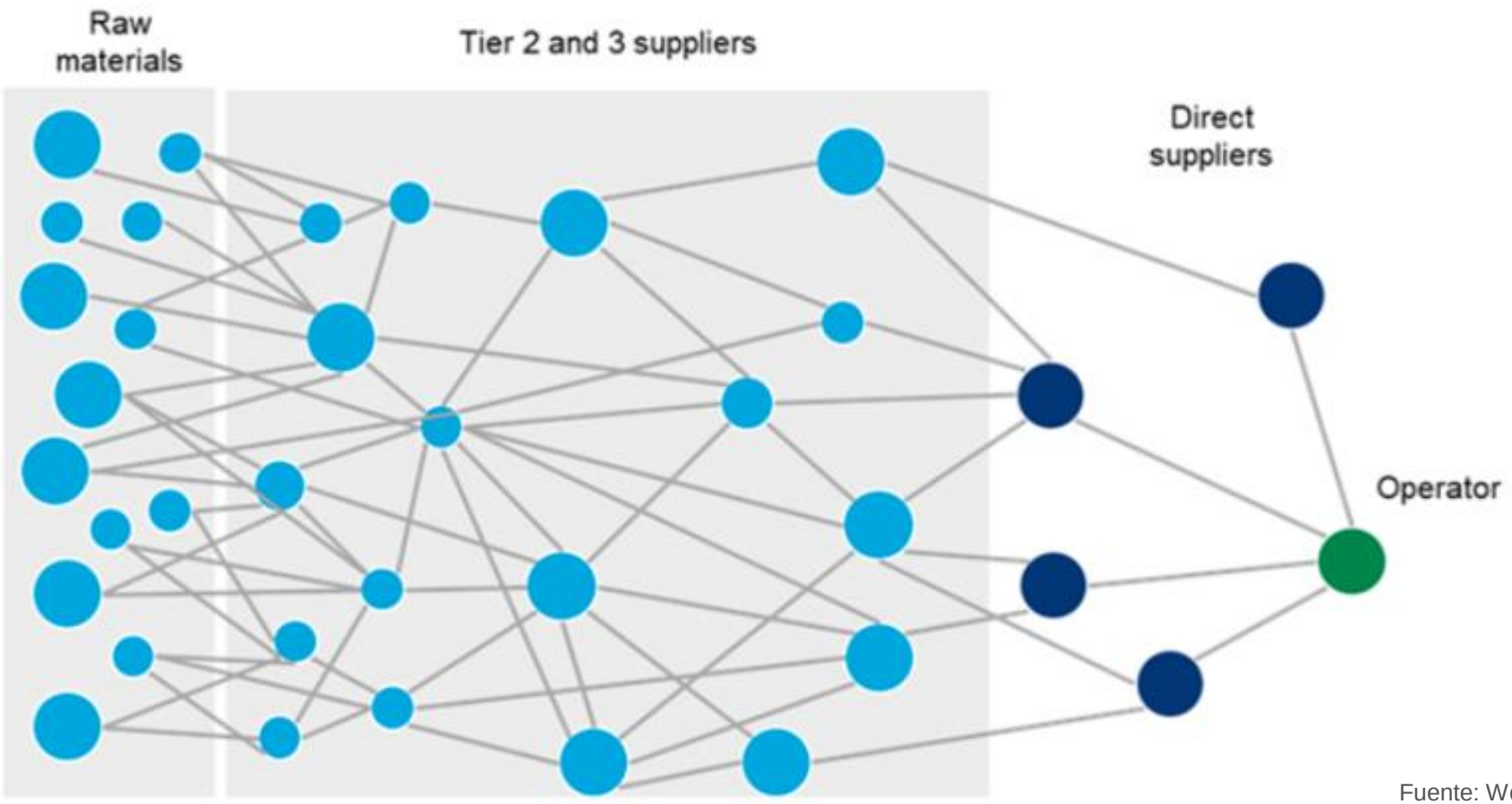
El ataque a manos de todos, pero, qué pasa con las capacidades para defenderse?



Sources: BCG *Navigating Rising Cyber Risks in Transportation and Logistics* (August 2021).

La cadena de suministros

Interconexión de actores

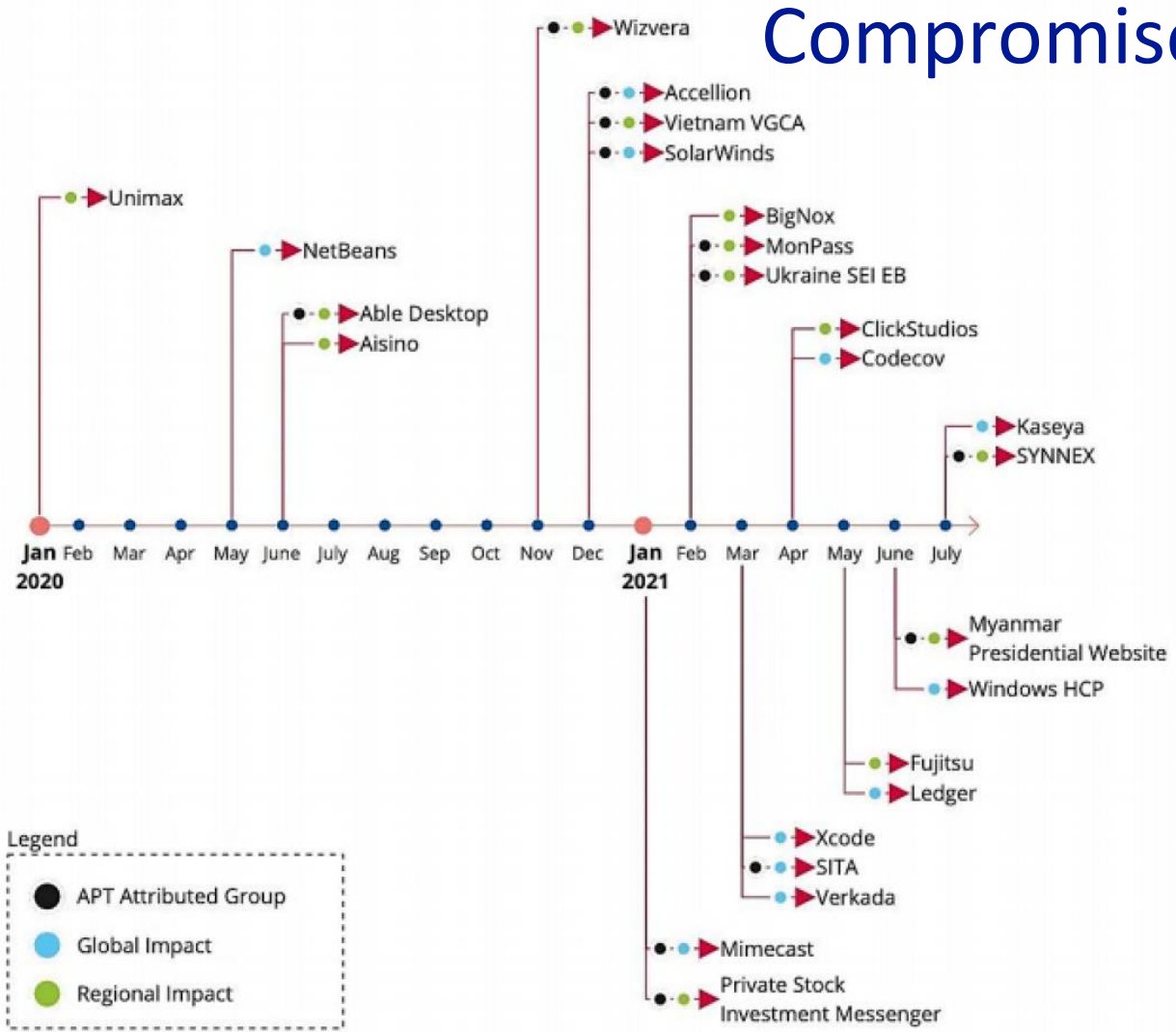


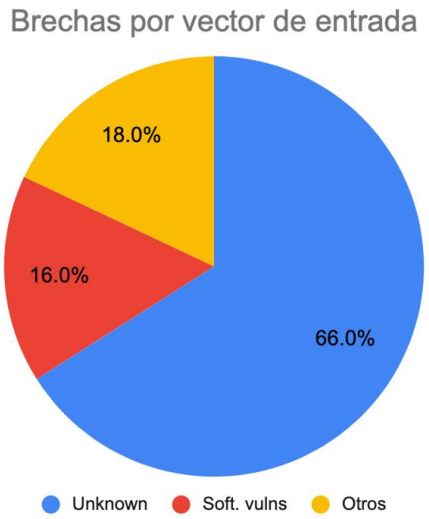
Fuente: Wood Mackenzie

La ciberseguridad en la cadena de suministros

- Amenaza a la que se enfrenta cualquier empresa en la actualidad
- Las organizaciones recién ahora están comenzando a comprender y gestionar el riesgo
- La falta de una estrategia de gestión de riesgo en este aspecto crea la oportunidad para una brecha, incluso con una sólida estrategia de gestión de riesgo “interno”.

Compromisos





Fuente: ENISA

Tres pilares a evaluar

- Los proveedores “escondidos”, con una higiene de seguridad deficiente que, una vez comprometidos pueden afectarnos.
- La falta de controles de seguridad en el hardware y dispositivos IoT conectados a la red.
- El software (garantías, vulnerabilidades, errores de diseño, etc)

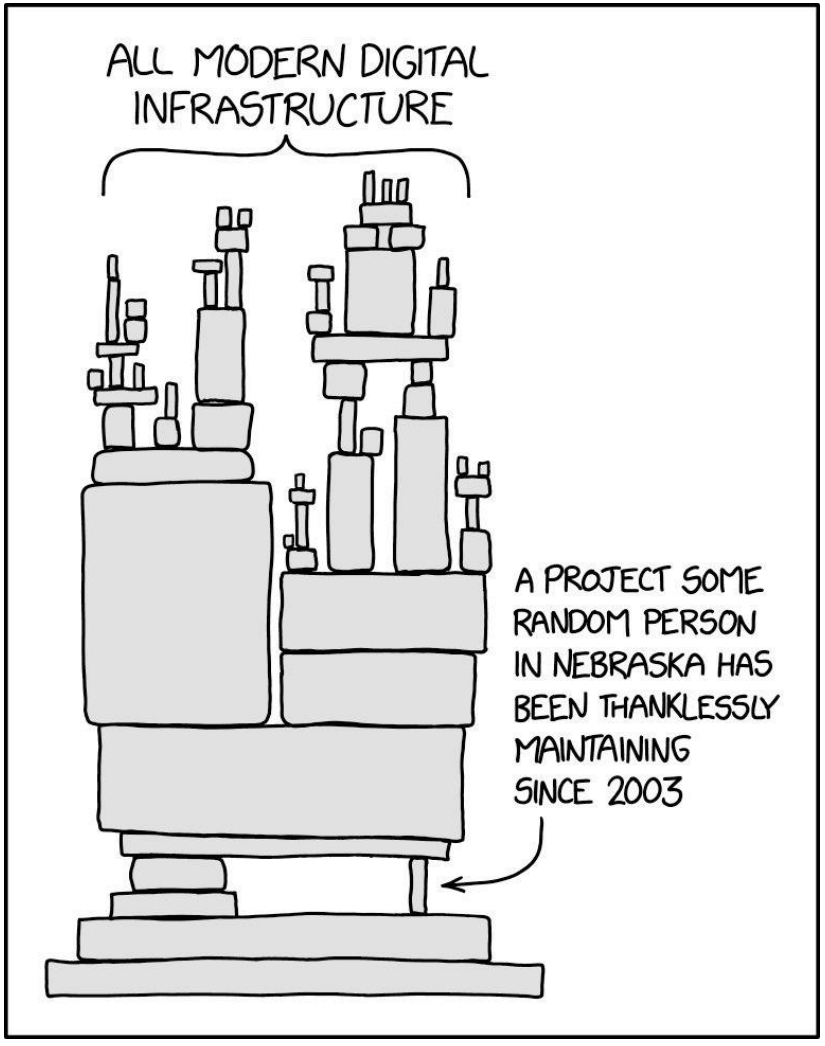
Ok, pero ¿qué podemos hacer?

Entender el entorno…

- Entender cuál es nuestro entorno y cuáles son las amenazas a las que estamos expuestos nos permitirá realizar mejores modelos de amenazas

- Adopción de nuevos paradigmas para controlar mejor la dispersión y alcance de un compromiso

- La pregunta, es cuándo nos va a ocurrir?



Los proveedores…

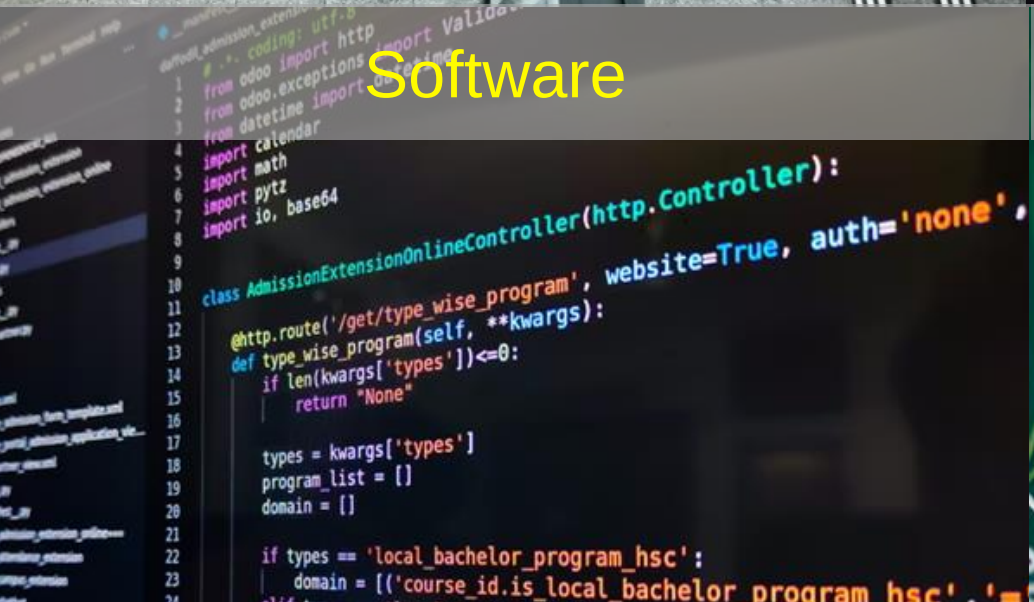
- Debemos entender las prácticas de gestión de riesgo de nuestro proveedores

- Debemos ir más allá y evitar caer en “eso ya será problema de ellos”

- Al introducir un nuevo proveedor en nuestra organización, debemos ser capaces de medir el riesgo que introduce.

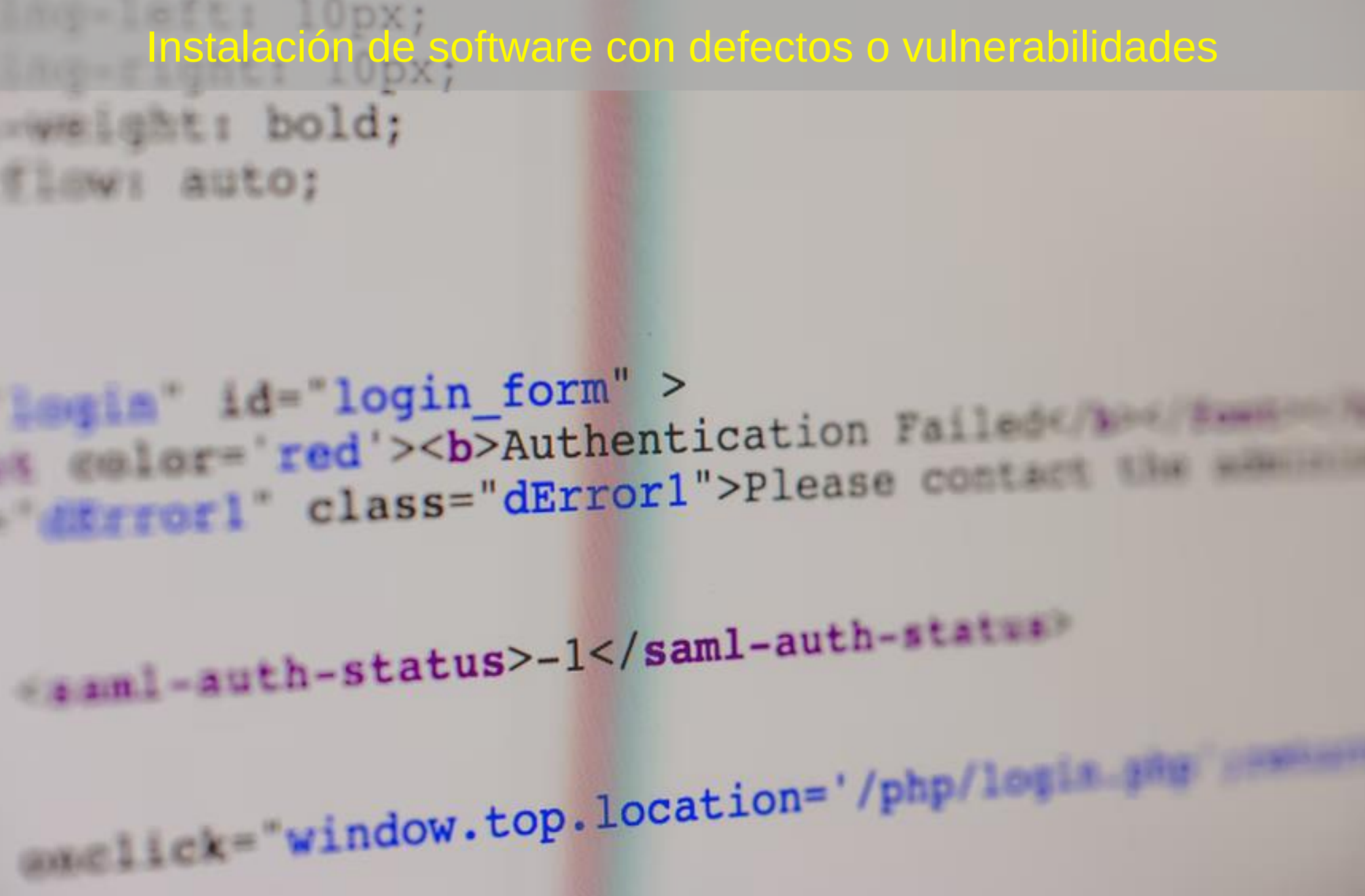
Personas

Servicios


Software
from odoo import http
from odoo.exceptions import Valida
from datetime import datetime
import calendar
import math
import pytz
import io, base64
class AdmissionExtensionOnlineController(http.Controller):
@http.route('/get/type_wise_program', website=True, auth='none',
def type_wise_program(self, **kwargs):
if len(kwargs['types'])<=0:
return "None"
types = kwargs['types']
program_list = []
domain = []
if types == 'local_bachelor_program_hsc':
domain = [('course_id.is_local_bachelor_program_hsc', '=

Hardware

Instalación de software con defectos o vulnerabilidades



Alteración o interrupción en la producción o distribución

¿Cuáles son los mayores desafíos?

- **Crear conciencia y una estructura adecuada**, a menudo se asigna la responsabilidad de la ciberseguridad al departamento legal o de TI
- Lograr una buena coordinación y comunicación con los stakeholders
- Definir un responsable de gestión para cada proveedor
- Incrementar la visibilidad
- Definir playbooks o planes de respuesta a incidentes de seguridad muy específicos o demasiado genéricos

Estándares y guías

- NIST C-SCRM y Cybersecurity Framework
- Charter of thrust
- Guías del UK's National Cyber Security Centre (NCSC)
- ISO: 27001, 27036 y 28000

Category	Baseline Cybersecurity Supply Chain Requirements [1)]
Data Protection	Products or services shall be designed to provide confidentiality, authenticity, integrity and availability of data
	Data shall be protected from unauthorized access throughout the data lifecycle
	The design of products and services shall incorporate security as well as privacy where applicable
Security Policies	Security policies consistent with industry best practices such as ISO 27001, ISO 20243, SOC2, IEC 62443 shall be in effect (including acc verification, encryption, network isolation/ segmentation, operational security, physical security, vendor management)
	Guidelines on secure configuration, operation and usage of products or services shall be available to customers
	Policies and procedures shall be implemented so as not to consent to include back doors, malware, and malicious code in products an
Incident Response	For confirmed incidents, timely security incident response for products and services shall be provided to customers
Site Security	Measures to prevent unauthorized physical access throughout sites shall be in place
Access, Intervention, Transfer, & Separation	Encryption and key management mechanisms shall be available, when appropriate, to protect data
	Appropriate level of identity and access control and monitoring, including third parties, shall be in place and enforced
Integrity and Availability	Regular security scanning, testing and remediation of products, services, and underlying infrastructure shall be performed
	Asset Management, Vulnerability Management, and Change Management policies shall be implemented that are capable of mitigatin
	Business continuity and disaster recovery procedures shall be in place and shall incorporate security during disruption, where applicab
	A process shall be in place to ensure that products and services are authentic and identifiable
Support	The timeframe of support, specifying the intended supported lifetime of the products, services or solutions shall be defined and made
	Based on risk, and during the timeframe of support, processes shall be in place for: (1) Contacting Support, (2) Security Advisories, (3) Cybersecurity related Patch Delivery and Support
Training	A minimum level of security education and training for employees shall be regularly deployed (e.g., by training, certifications, awaren

NCSC Supply chain security guidance	**Stage I** Understand the risks	1. Understand what needs to be protected and why	2. Know who your suppliers are - build an understanding of what their security looks like	3. Understand the security risk posed by your supply chain
	Stage II Establish control	4. Communicate your view of security needs to your suppliers	5. Set and communicate minimum security requirements for your suppliers	6. Build security considerations into your contracting processes and require your suppliers to do the same
		7. Meet your own security responsibilities as a supplier and consumer	8. Raise awareness of security within your supply chain	9. Provide support for security incidents
	Stage III Check your arrangements	10. Build assurance activities into your supply chain management		
	Stage IV Continuous improvement	11. Encourage the continuous improvement of security within your supply chain	12. Build trust with suppliers	

Para cerrar…

- Pasar a una postura de gestión de riesgo de la cadena de suministro más transparente, sostenible y apropiada para el negocio requiere:
  - Que la organización comprenda el riesgo que implica la cadena de suministros
  - Que la organización sepa como abordar ese riesgo y esté motivada
  - Que la organización comprenda que se requiere de una estructura adecuada para la gestión del riesgo de la cadena de suministros
  - Que la organización esté preparada para cuando algo falle y sepa como actuar

Nuestra seguridad, y la de nuestra cadena de suministro será tan fuerte como el eslabón más débil

DANKE!
THANK YOU!
MERCI!
GRAZIE!
GRACIAS!
DANK JE WEL!

. . . . . .

@fcm_uy