masempresas.cea.es
#masempresas

Ciberseguridad en tiempos de Covid-19

La excepción como instrumento de ingeniería social

Financiado por:

CEA
Confederación de Empresarios de Andalucía

Junta de Andalucía
Consejería de Transformación Económica, Industria, Conocimiento y Universidades

Fomento de la Cultura Emprendedora

Ponente: ***Nacho Barnés***

Dedicado a la técnica de sistemas durante 15 años, despierta el interés en el Análisis Forense hace cinco años, como parte de la actividad de respuesta ante incidentes.
En posesión de las certificaciones ECCouncil CHFI e IRCP de Securizame, instructor del EC Council y autor de cursos sobre forensia y respuesta ante incidentes para distintas plataformas online.
Actualmente, Director Técnico de Ciberseguridad en Arelance, consultora tecnológica malagueña con más de 15 años de experiencia, especializada en ayudar a tomar el camino más apropiado para lograr la Transformación Digital de tu organización, poniendo en marcha, a través de sus especialistas y servicios adaptados, soluciones integrales, soporte a proyectos y formación TIC, con un equipo de expertos en las áreas de formación, selección, tecnología de la información, recursos humanos, compuesto por más de 200 profesionales, que combinado con la experiencia acumulada desde 2003, ofrecen a las organizaciones, soluciones tecnológicas a medida de sus necesidades.

arelance
Building Digital Talent

Agenda

- Introducción. Ciberseguridad y ciberdelincuencia
- Ingeniería social, ¿de qué hablamos?
- Ejemplos de campañas durante la pandemia
- Fuentes de información fiables. Buscando ayuda
- Ciberseguridad y teletrabajo. Mejores prácticas
- Recursos online de interés para el teletrabajador

Introducción. Ciberseguridad y ciberdelincuencia

Algunos datos….

- El negocio del cibercrimen es un negocio al alza, que mueve del orden de 1,5 billones de dólares como volumen de negocio.
- Adicionalmente, aporta un riesgo empresarial estimado en 6.000 millones de dólares.
- Se encuentran del orden de 400.000 nuevas muestras de malware diarias.

Introducción. Ciberseguridad y ciberdelincuencia

Algunos datos….

- En España, el uso de Internet alcanza al 91% de la población, incluyendo la aceleración provocada por el estado de alarma.
- En cuanto a ciberseguridad, "*el 23 % de las empresas grandes en España ha sufrido algún incidente de seguridad durante el último año. En el caso de las PYMES el porcentaje baja hasta el 12 % y en el caso de ciudadanos sube hasta situarse en el 28 % por debajo de la media europea que se sitúa en el 34 %".*

Fuente: Ciberamenzas y tendencias, Ed.2020. CCN

Introducción. Ciberseguridad y ciberdelincuencia

Algunos datos….

- Entre los agentes de amenaza, encontramos:
  - *Estados y grupos patrocinados por estados. (p.e. APT28). La influencia como motivación emergente.*
  - *Ciberdelincuentes. El ransomware, la otra pandemia. Fraude del CEO.*
  - *Ciberterroristas. Sin demasiada capacidad operativa, centrados en la coordinación y el reclutamiento.*
  - *Hacktivistas (p.e. Anonymous, La9deAnon), cuya finalidad es la visibilidad y la protesta.*
  - *Insiders, intencionados o no. Concienciación.*

Fuente: Ciberamenzas y tendencias, Ed.2020. CCN

Introducción. Ciberseguridad y ciberdelincuencia

Algunos datos….

- En 2019, el CCN-CERT:
  - *Gestionó 42.997 ciberincidentes.*
  - *De los cuales, 3.200 fueron de peligrosidad muy alta o crítica.*
  - *El CERT explica esta criticidad como incidentes que pueden llegar a afectar a nuestro modo de vida.*
  - *La cibercriminalidad en España, representa un 10% del total de infracciones penales, según el sistema estadístico de criminalidad, SEC.*

Ingeniería Social, ¿de qué hablamos?

Ingeniería social. Definición.

"Cualquier acción que induce a una persona a realizar algo en interés del inductor"

"Y habitualmente en contra de los intereses de la persona"

https://www.social-engineer.org/framework/general-discussion/social-engineering-defined/

Ingeniería Social, ¿de qué hablamos?

Ingeniería social.

- En este panorama, la ingeniería social es uno de los principales vectores de entrada, con distintos fines:
  - Obtención de datos, en un mundo dónde los datos son el “nuevo oro”.
  - Provocar ejecución de malware.
  - Estafa “burda”, como el fraude al CEO o las llamadas de falsos empleados de Microsoft. Vishing.
  - El correo electrónico es la principal vía de llegada al usuario, phishing y spear-phising.
  - Si el medio empleado es el sms, se llama smishing.

Ingeniería Social, ¿de qué hablamos?

¿Cómo detectar el uso de ingeniería social?

- La urgencia es un indicador común.
- La ventaja económica, descuentos ligados a un corto plazo de tiempo, solicitud de cantidades ínfimas de dinero.
- Errores ortográficos o de redacción.
- Información poco inteligible para el usuario medio.

En general, si no es una comunicación esperada y/o solicitada, comprueba.

Ingeniería Social, ¿de qué hablamos?

Fraude del CEO

Ingeniería Social, ¿de qué hablamos?

Particularidades en el entorno de la COVID-19

- Apertura de las empresas de forma precipitada al teletrabajo:
  - Ver shodan.io con escritorio remoto.
- Foco de los ciberdelincuentes en las herramientas “estrella”, como son VPN’s, Zoom, servicios en la nube.
- Objetivo en las redes de los teletrabajadores, como vía de entrada a las redes corporativas.
- Mayores esfuerzos en espionaje industrial a farmacéuticas.
- Aparece como objetivo la cadena de producción, siendo el entorno industrial un sector carente de cultura en Ciberseguridad.

Ejemplos de campañas durante la pandemia

Algunos ejemplos:

- https://www.eleconomista.es/ecomotor/trafico/noticias/11016644/01/21/Nueva-alerta-de-phishing-la-DGT-no-envia-multas-de-trafico-por-correo-electronico.html
- https://www.eleconomista.es/nacional/noticias/11117263/03/21/La-campana-de-phishing-que-suplanta-a-Netflix-para-robarte-los-datos-bancarios.html
- https://maldita.es/malditobulo/cuidado-el-sms-que-te-pide-1-euro-en-tasas-de-aduanas-despues-de-que-no-te-hayan-podido-entregar-un-paquete-no-es-de-correos-es-un-timo
- https://www.elcomercio.es/sociedad/falsa-llamada-los-tecnicos-microsoft-nueva-estafa-sobre-que-alerta-guardia-civil-20200909100333-nt.html?ref=https%3A%2F%2Fwww.google.com%2F
- https://www.elcomercio.es/sociedad/alerta-estafa-utiliza-netflix-suscripcion-gratuita-robar-datos-guardia-civil-whatsapp-aislamiento-coronavirus-20200326171737-nt.html
- https://www.itdigitalsecurity.es/endpoint/2020/07/los-ataques-relacionados-con-covid19-llegaron-a-superar-los-200000-semanales
- https://www.itdigitalsecurity.es/endpoint/2020/08/el-uso-de-senuelos-de-ingenieria-social-ha-alcanzado-otro-nivel-con-la-pandemia
- https://theconversation.com/ciberataques-durante-la-crisis-de-covid-19-por-que-picamos-134814

Ejemplos de campañas durante la pandemia

Algunos ejemplos:

Estimado cliente,

Hemos detectado un **intento de fraude por email a clientes de Iberdrola**, por parte de una entidad desconocida. Un posible remitente es clientes930@iberdrola.cz, aunque podría haber otros. Cada vez es más frecuente recibir ataques de phishing y queremos ayudarte a identificarlos.

¿Sabes en qué consiste el phishing? Es un tipo de fraude online en el que los ciberdelincuentes se hacen pasar por compañías de tu confianza mediante SMS, correo electrónico o redes sociales para pedirte información confidencial. Puedes verlo en este vídeo:

¿Qué tienes que hacer si recibes un mensaje de Iberdrola o de cualquier compañía que te resulte extraño?

Verifica que la dirección de correo se corresponde con la compañía que lo envía	**Si el mensaje es urgente o te ofrece una ganga, desconfía**	**Si te piden información personal, desconfía**	**Comprueba que la web a la que te dirige el link es auténtica**

Fuentes de información fiables. Buscando ayuda

Fuentes de información gubernamentales

El centro Criptológico Nacional es el centro de excelencia en materia de ciberseguridad. Enfocado a la administración pública e infraestructuras críticas. Ver informes públicos y guías.

https://www.ccn-cert.cni.es/

El Instituto Nacional de Ciberseguridad, INCIBE, se enfoca a pymes, desarrollo de la cultura de Ciberseguridad y apoya al usuario en el ámbito particular. Dispone de varios portales y se le puede contactar a través del 017. Es importante reportar los casos que podamos encontrar. Es como los baches de la carretera, no vale el “otro lo hará”.

https://www.incibe.es/

Fuentes de información fiables. Buscando ayuda

Fuentes de información gubernamentales

La agencia Española de Protección de datos también provee de información muy interesante en la materia.

https://www.aepd.es/es

Y las FCSE, como no puede ser de otra manera….

https://www.gdt.guardiacivil.es/webgdt/cusuarios.php

https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php#

Ciberseguridad y teletrabajo. Mejores prácticas

Medidas de seguridad:

Veamos estos artículos de Incibe:

https://www.incibe.es/protege-tu-empresa/blog/pautas-ingenieria-social-covid-19

https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo

¿Sabemos comprobar un domino?. Ejemplos…

1. Protocolo
2. Subdominio
3. Dominio
4. TLD (Top Level Domain) o extension
5. Subcarpeta o directorio
6. Archivo

Podemos consultar datos de propiedad en:

https://whois.domaintools.com/

Ciberseguridad y teletrabajo. Mejores prácticas

Consejos:

Podemos encontrar distintas guías y fuentes de información:

https://www.ccn-cert.cni.es/cibercovid19/teletrabajo.html

Otros posibles….

- Utilizar un **antivirus de confianza y actualizado**.
- Mantener **actualizados los sistemas operativos y los navegadores.**
- Comprobar el tipo de conexión segura/insegura, así como desconfiar de URL's raras.
- No bajar la guardia. **No todo el Malware es conocido por los antivirus. (Menos del 40%).**
- Usar siempre una cuenta **de usuario con permisos restringidos,** evitando usar la cuenta de administrador. Nos deshabilitar el UAC de Windows y desconfiar de aquellos programas que nos piden elevación de privilegios sin esperarlo.

Ciberseguridad y teletrabajo. Mejores prácticas

Consejos:

- **Utilizar contraseñas robustas** y distintas para cada uno de los servicios de Internet que utilicemos, así como segundo factor.
- **Desconfiar** de los enlaces o descargas que nos aparecen en páginas web de poca confianza. Si nosotros quisiéramos distribuir un Malware que la gente se instalase de forma voluntaria, ¿Qué haríamos?. No dejarnos conducir.
- No hacer operaciones bancarias **desde ordenadores que no sean de tu confianza.** Lo ideal sería utilizar un ordenador específico para “operaciones sensibles” en la Red y no mezclar la navegación de ocio.
- Ser muy cautelosos con la información **que se decide compartir en la Red** y con quien se comparte, porque Internet es como Las Vegas, **lo que se sube a Internet queda en Internet** y no será fácil su borrado total.

Y por encima de todo, mantener una actitud de alerta frente a cualquier indicio o sospecha. Por defecto, desconfiar…

Recursos online de interés para el teletrabajador

Algunos enlaces:

En caso de verse afectado por ransomware:

https://www.nomoreransom.org/

Para comprobar un fichero o una url en busca de malware:

https://www.virustotal.com/gui/

Para ver si mis datos han sido comprometidos:

https://haveibeenpwned.com/

Comprobación de puertos abiertos en mi conexión:

https://www.internautas.org/w-scanonline.php

Reportando un incidente de seguridad:

https://www.incibe.es/protege-tu-empresa/reporte-fraude

Información y Consultas en
masempresas.cea.es

/CEA.es @CEA.es_ /CEA.es

Gracias

Financiado por:

CEA
Confederación de Empresarios de Andalucía

Junta de Andalucía
Consejería de Transformación Económica, Industria, Conocimiento y Universidades