INSTITUTO TECNOLÓGICO DE
TLALNEPANTLA

TECNOLÓGICO NACIONAL DE MÉXICO

INSTITUTO TECNOLÓGICO DE TLALNEPANTLA

INGENIERIA EN TECNOLOGÍAS DE LA INFORMACIÓN

Relatoría

MATERIA: TECNOLOGÍAS DE SEGURIDAD EN SOFTWARE

ALUMNO: ALCANTARA SALAZAR JOEL

No. DE CONTROL: 16251053

PROFESORA: DÍAZ RINCÓN HILDA

FECHA: 05-09-2021

Contenido

Introducción

La siguiente relatoría habla sobre una pequeña presentación que un hombre llamado Juan Pablo Castro que es director de innovación tecnológica en TREND MICRO nos da, hablando sobre temas de ciberseguridad en el año 2021.

Este experto nos da algunas pequeñas predicciones de ataques que sucederán este año, todo esto consecuencia de la nueva normalidad en la que nos encontramos, ya que bien sabemos que la pandemia es un tema que vino a cambiarnos la vida, y todos (incluido los cibercriminales), nos hemos tenido que adaptar para que el mundo empresarial no se detenga y entremos en un gran colapso.

Habla principalmente en como nuestros hogares serán los próximos centros de los ataques, y de igual forma como lo relacionado con la salud publica será el nuevo blanco. Se platica que las vacunas contra el covid son los nuevos activos que debemos de cuidar a capa y espada, ya que de ello dependen vidas.

Espero que con mucha atención podamos darnos cuenta que uno de los problemas principales es la ignorancia de nuestra población a los temas de ciberseguridad, de igual modo aquí hay algunos tips con los que podemos empezar a nutrirnos de esta información.

Por ultimo cerramos con las preguntas y respuestas que este dio al público, algunas no muy relevantes para el tema de seguridad, pero que sin duda nos dan una gran enseñanza y nos dejan mucho que pensar.

¿Qué nos espera en ciberseguridad en este 2021?

La webinar comienza dando la bienvenida y dando una pequeña introducción sobre lo que tratara, además, presento a Juan Pablo Castro (director de innovación tecnológica en TREND MICRO) persona que lo acompañara durante dicha presentación.

Predicciones de seguridad para 2021 (Juan Pablo Castro) Trend Micro.

Los cibercriminales convertirán las oficinas del hogar en sus nuevos centros criminales:

- Los equipos de TI necesitan proteger toda la fuerza de trabajo remota: Se habla de que esto es un cambio, en cual tenemos que aprender a proteger todos los equipos que trabajan en zona remota. No solo los equipos de cómputo, también la red que lo conecta
- Los routers domésticos serán un nuevo objetivo: Estos router se convierten en un punto de salida o un DNS de muchas peticiones, esto es lo que los hace tan apetecibles a los cibercriminales.
- Vulnerabilidades de VPN será un impulsor de nuevos ataques remotos: Nos comenta Juan Pablo que a pesar de que las VPN hoy en día ya no son tan utilizadas, de igual modo existe un alto riesgo de ataque, sobre todo a los clientes de dicha red que se ocupan de la administración de la empresa, como: los encargados de finanzas, RH, etc. Muchas veces estos datos son extremadamente críticos, por lo que el riesgo sigue siendo muy crítico.
- Los cibercriminales saltaran de la maquina de un empleado remoto a otro hasta que encuentren a un objetivo adecuado: Mediante las credenciales de acceso es como ellos pueden llegar hasta los altos cargos sin hacer mayor esfuerzo.

- Ataques de robo de datos contra empleados de confianza (RRHH, Finanzas, Logística, Pagos, Legal) que acceden de forma remota a información confidencial y critica: Adicionalmente ellos hacen
- El acceso como servicio como modelo de negocio lucrativo para los delincuentes que buscan vender acceso a enrutadores domésticos comprometidos y redes convergentes de TI / TO, también se vende el acceso a redes empresariales: Nos relatan que este tipo de cibercriminales su tarea es entrar a la red del lugar objetivo, mantenerse y por ultimo vender el acceso, ellos pueden mantener el acceso durante meses, es el tema que tenemos que tener más en cuenta

La temática de la pandemia Covid-19 será la prioridad número uno de los equipos de ciberseguridad, ya que demuestra ser un terreno fértil para campañas maliciosas

El uso de señuelos con el tema del coronavirus es un tema que ya paso de moda, según la platica tenemos que tener en cuenta siempre que la temática cambie, en esta ocasión hablamos sobre la pandemia, pero siempre el tema de moda será motivo de engaño. Aquí vemos algunas características de este modo:

- Los ciberdelincuentes seguirán activos en el tema de señuelos acerca de coronavirus, especialmente focalizados a las vacunas y campañas de vacunación: Un ejemplo dado es que dicen que la empresa compro tantas vacunas, y para poder obtenerla debes de registrarte en algún link desconocido. Ese es el tema principal con esta modalidad, saber cuando tu empresa esta de verdad llevando una campaña y estar siempre bien informado de el modo que esta se aplicará.
- Sabotaje de la producción, el trafico y el transporte de productos falsificados surgirán como modus operandi delictivos en medio de la pandemia: Este tema como un circulo malicioso de robo, hay personas que entran en los sistemas de logística (sobre todo de negocios en línea, como Amazon) para saber cuando y que transportaran los vehículos de dichas empresas. Esta

información sabemos que es muy importante para algunas otras personas que igual se dediquen a hacer cosas malas y puedan sacar gran provecho de esto.

- Los sistemas de seguridad sanitaria deben abordar los riesgos de seguridad asociados con los datos de los pacientes, los ataques de malware y el espionaje médico.
- Los criminales intentaran obtener inteligencia sobre las cadenas de logística de distribución y robar la investigación de vacunas: Si bien no tengo idea de la fecha en que se llevó esta conferencia. Es un hecho que el robo de inteligencia sobre la distribución e investigación de las vacunas comenzó desde el momento que EEUU anuncio su primera vacuna. La carrera por ver quien era el primer país en venderla fue el tema principal durante el inicio de la pandemia, pero de igual modo esto se nos relata como una predicción debido a que es un tema que aun seguirá por algunos años hasta que la mayor parte de la población mundial estén vacunados.
- El ataque a las cadenas de frio de almacenamiento de vacunas: Aquí se toco un tema bastante interesante ya que nos comentaba que la mayoría de los ataques de ramsonware se han realizado a hospitales, por el tema de que ahí se manejan vidas, y el tiempo que se tarden en poder registrar a un paciente o saber su información clínica puede costarle la vida. Esta predicción hace alusión a ese rapto de control de algunos equipos que mantengan vivas las vacunas, e caso de negarse a pagar el rescate, podrán hacer que miles de vacunas mueran, lo cual también tomara muchas vidas.

El tele trabajo obligará a las organizaciones a enfrentarse a entornos híbridos y arquitecturas de seguridad insostenibles.

El tema sobre el teletrabajo me parece interesante, por que si bien, algunas empresas se han beneficiado de esto, la adaptación a hacerlo de dicha manera ha sido mas desafiante de lo planeado. Nos dice que las organizaciones tienen menor control sobre el uso de los datos que hacen los empleados y tienen una menor

visibilidad en entornos híbridos. Lo cual me hizo recordar el trabajo que me costo inscribirme a este semestre, ponerme de acuerdo con la coordinadora y otras dependencias y a su vez estas mismas se comunicaran fue un tema que se prolongo casi dos semanas.

Una de las medidas de las organizaciones para defenderse de es adoptar un modelo de confianza, nos da un ejemplo especifico que es Zero Trust, según el sitio web **ciberseguridad.blog** "*El modelo de seguridad de Zero Trust asume que los actores que no son de confianza ya existen dentro y fuera de la red. Por lo tanto, la confianza debe ser completamente eliminada de la ecuación. Zero Trust Security requiere poderosos servicios de identidad para asegurar el acceso de cada usuario a las aplicaciones e infraestructura*." (Ramiro, 2019)

En palabras simples, nos dice que Zero Trust actúa como el guardia de seguridad de un fraccionamiento, el cual pide específicamente que vivas ahí, y aun así vigila que no haya intrusos, debido a que el modelo Zero Trust tiene cero confianzas, tanto de dentro, como de fuera. Este modelo se ha convertido en el favorito de las corporaciones que han tenido que cambiar su modo de trabajo por cuestiones de pandemia.

Por ultimo (hablando sobre los modelos híbridos) se habla sobre como la fuerza de trabajo remota con aplicaciones y software de seguridad desactualizado será un objetivo para los cibercriminales debido a que muchos de estos trabajadores suelen mantener cierta indiferencia hacia los modelos de seguridad y como las actualizaciones de esto les puede ayudar. Para los cibercriminales esto seria un gran banquete, ya que podrían entrar a cualquier parte si problemas.

Los atacantes utilizarán rápidamente las vulnerabilidades recién descubiertas, dejando a los usuarios con una ventana estrecha para colocar los parches de seguridad.

La adopción rápida de vulnerabilidades y exploits de día n (n-day): Hemos escuchado mucho sobre los exploits de día cero, pero este ataque no habla de eso,

habla sobre lo que pasa después del día 0 (de ahí el nombre), descubiertos específicamente en herramienta y plataformas.

Lo que evidentemente abrió un nuevo mercado, donde los cibercriminales venden errores conocidos explotables, con posibilidad de personalización de día n. Con la personalización de los exploits es mucho más difícil poner un parche a la falla, como dice el nombre, se hace a medida se ejecuta y se explota, por eso para los delincuentes es muy importante la auto critica, para seguir explotando dichas fallas.

Hablando sobre la personalización, se nos platica sobre el mayor uso y automatización de herramientas de prueba de penetración, incluido Cobalt Strike

¿Qué es cobalt strike?

2012, Cobalt Strike se ha utilizado como una forma proactiva de probar las defensas de la red contra herramientas, tácticas y procedimientos (TTP) avanzados de actores de amenazas.

El objetivo, por supuesto, es imitar a los actores de amenazas más maliciosos y sus técnicas para probar su postura de seguridad y practicar los procedimientos de respuesta. Desafortunadamente, como la mayoría de las cosas en seguridad, las herramientas y el conocimiento destinados a ayudar a los equipos de seguridad también pueden ser utilizados de forma maliciosa por los delincuentes. (Seguridad, 2020)

El fragmento de este artículo, combinado con lo que nos platica Juan Pablo, nos dice como esta herramienta se ha convertida en la favorita por los cibercriminales para efectuar ataques y de forma silenciosa conocer las vulnerabilidades de alguna red. Y no se trata de saber que te están atacando con cobalt Strike, si no que estos delincuentes personalizan el ataque haciendo más difícil su detección.

Como última opción de este tema volvemos a tocar el tema de la venta de conocimiento adquirido como herramientas para ataques futuros, lo que nos regresa a este circulo vicioso de compra y venta de información a, incluso, competidores directos.

Las APIs expuestas serán el próximo vector de ataque para las brechas empresariales

Nos platican de un hecho que pareciera a simple vista demasiado obvio, pero que pocas veces les prestamos atención. El hecho de trabajar con APIs de otros desarrolladores nos hace vulnerables a sus vulnerabilidades, y como dice el famoso dicho "*una cadena es tan fuerte como su eslabón mas débil"* esto nos hace susceptibles a múltiples ataques sin que nos demos demasiada cuenta.

En este tema nos explican con el ejemplo de un mesero cual es la función de una API, en el cual nos dicen que cada API tiene una función en especifico y solo puede cumplir esas tareas para lo que están hechas, y si bien, son demasiado útiles cuando desarrollamos una aplicación y tenemos que usar, quizá, algunas funciones, que, valga la redundancia, no sabemos como funcionan, pero ya están hechas y listas para que las agreguemos a nuestro programa. Eso es una API, el ejemplo mas claro son los mapas de Google, si uber quisiera tener su propio servicio de mapas, tendría que hacer toda la labor que Google ya hizo antes, como conocer todas las calles y lugares de la tierra. Así mismo si tu quieres hacer una tienda en línea, tendrás que utilizar las APIs de los bancos y así se va juntando la cadena, y de ese modo hay millones de APIs conviviendo en este segundo.

Juan Pablo es muy claro sobre la complejidad que llegan a tener ciertas aplicaciones que utilizan multiples APIs, incluso nos reta a decir si nosotros no convivimos con ellas (lo cual es evidente que todos convivimos con ellas), pero es muy tajante en decir que este tipo de arquitectura puede mostrar problemas mas claros de lo que podríamos llegar a pensar y los enlista de la siguiente manera:

- **Velocidad:** La mayoría de estas se alojan en la nube y se comunican públicamente mediante internet
- **Complejidad**
- **La falta de visibilidad**
- **Múltiples nubes**

- Las interfaces de programación de aplicaciones (API) servirá como puntos de entrada a las redes de las organizaciones: Sin saberlo muchas de estas aplicaciones dan entrada directa a la red y el único modo de que esto no pase es asegurarnos que el desarrollador en cuestión haya sido cauteloso con su seguridad

- Las APIs son fáciles de descubrir y su seguridad es algo que recién se comienza a explorar: Como ya habíamos comentado, en un principio se hacían con la intención de cumplir una tarea especifica, ahora tenemos que cerciorarnos de que no volvamos vulnerables a nuestro programa o a quien quiera utilizarnos.

- El incremento en la velocidad repentina del desarrollo de APIs debido a la agilidad de la transformación digital dejara expuestas malas practicas y los fallos de configuración de infraestructuras de nube.

- El incremento de uso de APIs en infraestructuras de nube: Si hablamos de APIs, hablamos de nube, sabemos que la mayoría se almacena y se ejecutan a través de este servicio, lo que lo hace propenso a múltiples ataques a cualquier hora del día

Las aplicaciones de colaboración empresarial y las aplicaciones en la nube utilizadas para el trabajo remoto serán puestos a prueba en la búsqueda de vulnerabilidades criticas

Si esta clase fuera una empresa y necesitáramos compartir nuestra información importante a través de alguna plataforma, este seria el punto donde los criminales atacarían, a que me refiero con esto, Juan Pablo habla sobre que se buscaran vulnerabilidades criticas en aplicaciones comerciales, y la aplicación comercial que mas utilizamos son: Microsoft Teams y Moodle, y ya si nos ponemos un poco mas estrictos, nos damos cuenta que la plataforma donde los profesores suben evaluaciones y esta la información de los estudiantes de la escuela, el SII, es

altamente vulnerable, ya que esta hecho con tan poca cautela y dedicación, que seria muy fácil romperla y entrar. Y de esto es lo que habla específicamente esta predicción, la cual es insistir en que todas las aplicaciones que nosotros utilizamos para compartir información son el punto vulnerable que los atacantes desean, ya que incluso ahí mismo podrían encontrar como se hablan de las vulnerabilidades que se buscan erradicar.

Estrategias de ciberseguridad con miras al 2021

- Fomentar la educación y formación de los usuarios: Esto sabemos que es primordial y repetitivo, pero siempre debemos de mantener la cultura de seguridad en nuestros empleados y que no piensen que esto puede ser pasajero. Los usuarios deben de estar actualizados de las tácticas de los cibercriminales.
- Mantener un estricto control de acceso en la red corporativa y los empleados remotos trabajando desde su oficina en la casa. Crear políticas basadas en la seguridad y un plan de respuesta a incidentes que cubra todas las operaciones, en sitio y remotas
- Reforzar las medidas de seguridad básicas y los programas de gestión de parches y vulnerabilidades. Siempre actualice en instale parches a aplicaciones y sistemas con regularidad
- Evaluar diariamente las configuraciones de nube siguiendo las buenas practicas del proveedor de nube y normas de seguridad

Cibe-resiliencia

La ciber-resiliencia es un nuevo concepto que nunca había escuchado, pero suena bastante coherente si queremos crecer como organización, nos hablan de que debemos estar listos para crecer y domar las amenazas que nos puedan surgir, textualmente la ciber-resiliencia lo dictan de la siguiente manera "*Se refiere a la capacidad de una entidad para ofrecer continuamente el resultado esperado, a pesar de los eventos cibernéticos adversos.*

La ciber-resiliencia ayuda a las empresas a reconocer que los cibercriminales tienen la ventaja de las herramientas innovadoras, el elemento sorpresa, el objetivo y pueden tener éxito en su intento. Este concepto ayuda a las empresas a prepararse, prevenir, responder y recuperarse exitosamente al estado seguro deseado. Se trata de un cambio cultural, ya que la organización ve la seguridad como un trabajo de tiempo completo y las mejores practicas de seguridad integradas en las operaciones diarias. En comparación con la ciberseguridad, esta requiere que la empresa piense de manera diferente y sea mas ágil en el manejo de ataques".

La diferencia entre la ciberseguridad y la ciber-resiliencia radica en que una es una materia que debemos adoptar para proteger nuestros datos y la ciber-resiliencia es la capacidad o el empeño que vamos aponer para que esto se lleve a cabo de manera adecuada, si no estamos dispuestos a salir del hoyo, la tierra nos cubrirá.

Preguntas y respuestas

Pregunta: Anónimo

¿Cuál es tu perspectiva sobre los riesgos de las clases online, principalmente por la información de los niños?

Habla principalmente sobre lo poco capacitado que están algunos profesores sobre como utilizar dichas plataformas para compartir información. Pero nos da la recomendación de siempre mantener actualizado los clientes, o los software que utilizamos para nuestras clases, y especial énfasis en mantener educada a la población en general sobre temas de ciberseguridad, ya que aun no existe la cultura de hablar de esto siendo una época en donde convivimos diariamente con estas nuevas tecnologías.

¿Ahora whatsapp podría considerarse una API maliciosa?

Si bien whatsapp no es un API, de igual manera puede ser mal utilizada para enviar trampas por internet, aunque a lo que se hace referencia cuando se hablo de las APIs es a las que se encarga de interconectar servicios. Pero igual podría ser una API maliciosa

¿Crees que siga siendo tendencia los ataques de DDoS?

Dice que básicamente y dependiendo del propósito del criminal es que se utilizará este tipo de ataques, siendo tendencia o no. Pero explica que muchas veces este tipo de ataque es solo una distracción.

¿Con la nueva reforma de teletrabajo en México, crees que este vino para quedarse?

En su opinión personal dice que el teletrabajo llego para quedarse, ya que hace mas amplio el panorama incluso haciendo mas funcionales a ciertos trabajadores.

¿Hay alguna tendencia de seguridad para prevenir filtraciones en escenarios virtuales?

La virtualización y la nube tiene aspectos que se han dejado de lado, y son las redes, estas existen, y pensar en proteger la arquitectura sin cuidar las redes es un gran error.

Conclusión

Es muy difícil pensar que algunos de estos temas puedan pasarnos, pero de las palabras de un experto suena más increíble pensar que esto ocurre millones de veces al día. Si bien no soy un trabajador de alguna corporación que comparte datos importantes entre empleado, si soy un blanco de ataques, y mi información personal es igual de valiosa. Es por esta razón que dicha presentación me abrió los ojos e hizo reflexionar sobre lo expuesto que estamos, el tema de las APIs me pareció especialmente importante porque nunca había visto de ese modo la forma que estamos a merced por la falla de algún tercero. Es por esto que mi conclusión es que sigamos manteniendo la guardia arriba ante cualquier hipotético ataque, y en la medida de lo posible, y como futuros ingenieros de TICs, mantener informado a nuestra gente cercana y comenzar a crear una cultura de ciberseguridad mas fuerte y así evitar lo que se pueda convertir en una catástrofe

Referencias

Ramiro, R. (14 de Junio de 2019). *ciberseguridad.blog*. Obtenido de https://ciberseguridad.blog/que-es-zero-trust-en-ciberseguridad/

Seguridad, N. 4. (25 de Septiembre de 2020). *Nivel 4*. Obtenido de https://blog.nivel4.com/noticias/cobalt-strike-el-nuevo-favorito-de-los-ciberdelincuentes/