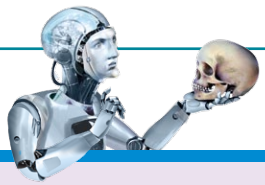

CAVILACIONES SEGURAS

Receta ¿magistral o mágica? para sobrevivir en 2021

Desde la humildad más absoluta, cual quiromante, me atrevo a compartir con vosotros mi propuesta de respuesta, que no previsión, ante el panorama de amenazas y ciberataques que se vislumbra para este recién estrenado año.

Existen fuentes con acceso a muchos más datos que quien os escribe desde esta columna, así que dejaré los IOCs ("indicadores de compromiso") a los informes sobre amenazas de proveedores que todos conocemos. El campo de batalla digital es cada vez más peligroso y, al mismo tiempo, más rentable para aquellos actores

"La teoría de juegos: la ciberseguridad es un juego asimétrico, no-cooperativo y de suma cero entre víctima y atacante; sin embargo, es un juego cooperativo y de suma no-cero entre compañías objetivo del mismo ataque"

del lado oscuro. En mi caso, comparto mis recomendaciones como una colección de punteros para eludir el fracaso (nótese que evito la expresión "conseguir éxito") en esto de la ciberseguridad.

Primero de todo, estimado colega, 2021 será un año en el que tu nivel de estrés puede aumentar por excesivas horas de trabajo y excesivo número de incidentes a responder. Sé selectivo en tus quehaceres. No olvides que tu salud, física y mental, el ejercicio físico y la alimentación son los pilares que te sostienen. Nuestra profesión viene acompañada de un alto grado de responsabilidad, complejidad y frustración: necesitarás de todo tu equilibrio interior para hacer frente a los desafíos profesionales.

Desde el punto de vista técnico, es importante pertrecharse con unas buenas fuentes de inteligencia: la de fuentes abiertas ("Open Source Intelligence") es una buena opción para comenzar. Necesitas conocer los detalles de los ataques más recientes que suceden en tu industria, en tu localización geográfica y en tu cadena de valor. Esto te permitirá enfocarte en prevenir y mitigar incidentes que suceden en la realidad. Normalmente estos son un subconjunto de todos los posibles. Recuerda que tus recursos limitados no te permitirán tratar todos los posibles incidentes que potencialmente puedan suceder. Por ello, una monitorización, que aprenda de esa inteligencia operacional, te permitirá identificar rápidamente los compromisos con destino a "las joyas de la corona" de tu compañía o cliente.

Desde el punto de vista estratégico, no descuides las vulnerabilidades más tradicionales en tu empresa o cliente: la gestión de identidades sigue siendo una de las más frecuentes. Si ya eres cliente o comienzas a ser usuario de proveedores de nube pública, recuerda que se externaliza el servicio pero no la responsabilidad. Preferiblemente, la gestión de identidades y de incidentes en la nube debería estar integrada con tus respectivos procesos internos.

Desde el punto de vista humano, vives en un mundo polarizado: mucho ruido y poca información destilada: piensa en usar nuevos métodos de comunicación distribuida, que no remota, con tus colegas, tus coordinadores y tus miembros del consejo. Este será probablemente tu mayor desafío. Siempre es posible perfeccionar nuestra expresión escrita y oral para desencadenar la respuesta óptima a la hora de explicar y mitigar un ciberincidente. Emplea distintas técnicas didácticas cuando necesites transmitir un mensaje eficazmente a los distintos tipos de receptores dentro de las organizaciones en las que participas.

Quizás sea ya el momento de evolucionar hacia un equipo de seguridad altamente pluridisciplinar... (algo que ya recomendaba en mi primer libro publicado en 2010), no sólo con técnicos en ciberseguridad, sino también con comunicadores, psicólogos, filósofos y demás representantes de otros campos de conocimiento que mejoren la visibilidad e impacto de tu equipo.

Construye también una colaboración efectiva con tus colegas en las empresas competidoras. Con tus rivales se batalla en producto y servicio pero no en información de seguridad. Recuerda la teoría de juegos: la ciberseguridad es un juego asimétrico, no-cooperativo y de suma cero entre víctima y atacante. Sin embargo, es un juego cooperativo y de suma no-cero entre compañías objetivo del mismo ataque.

En definitiva, estoy seguro de que 2021 viene cargado de emociones fuertes en el frente de las ciberamenazas. Sólo una visión holística y estratégica de nuestra función y de nuestro rol en las organizaciones nos puede dar las respuestas que necesitamos en este mundo ya tan complejo de navegar.

Concluyo animándote a conservar tu pasión por este campo profesional cuya relevancia no para de crecer y a dedicar algo de tu tiempo a formar a las nuevas generaciones de profesionales que, independientemente de su edad, se unirán a ti durante este nuevo año.

Alberto Partida
Analista en Ciberseguridad
itsecuriteer@gmail.com
@itsecuriteer en twitter
Sígueme en LinkedIn:
linkedin.com/in/albertopartida