EN MOMENTO DE CRISIS, MÁS INVERSIÓN PARA EVITAR RIESGOS GRAVES

Para muchos esta puede ser una frase impactante; para los que vivimos en el mundo de la seguridad bien sabemos que no.

La crisis ha transformado viejos riesgos en nuevos vectores de ataque que no solo suponen un riesgo operacional para las empresas sino que pueden afectar al valor de las mismas y a la visión que los clientes pueden tener sobre ellas. Durante este año hemos visto grandes corporaciones caer más de un 8% en bolsa debido a un fallo de seguridad que les obligó a cortar el servicio durante varias semanas, obligando a muchos de sus clientes a renovar sus tarjetas de crédito, ya que se habían visto comprometidas.

En el actual período de crisis económica se incrementan los riesgos intrínsecos derivados de cualquier actividad. Todos los sectores están afrontando una serie de ajustes presupuestarios que se están aplicando para obtener mayor eficiencia en los recursos, y la forma de aplicarlos nos debe diferenciar para salir victoriosos ante "el otro lado".

> Es vital que seamos cautelosos y nos mantengamos alerta ante los riesgos que el actual momento económico y social nos presenta. La obtención de beneficios rápidos por la industria del *malware* o la protesta social pueden convertirnos en el próximo objetivo.

La industria del *malware*

Si hemos utilizado muchas veces el término "industria del *malware*" es debido a la creciente industrialización y profesionalización de los procesos de desarrollo *malware*. Nuevos gestores de Botnet, CRM para comprobar la rentabilidad de los mismos, mercados de venta de datos de tarjetas de crédito... y otras actividades que a buen seguro verán la luz en los próximos meses.

Un momento como el actual es el caldo de cultivo idóneo para que los ciberdelincuentes intenten beneficiarse de las personas que sufren un mal momento con promesas de obtención de beneficios rápidos y sin esfuerzo.

Durante estos meses también hemos visto incrementarse las estafas derivadas de falsos programas antivirus o falsas páginas de búsqueda de trabajo y los ataques a través de redes sociales como Twitter y Facebook. Ninguno de nosotros pincharíamos en un link con este formato http://domain-book.ru/templates/ja_load/f.bin pero, ¿actuamos igual si vemos en un tweet conocido este enlace http://bit.ly/vieAOnla?

Estos movimientos son debidos a que la industria del *malware* vigila muy de cerca los movimientos empresariales y sociales, adaptándose a las circunstancias para mantener sus niveles de ingresos.

El descontento social y los grupos organizados

Por otro lado, tenemos antiguos ataques de denegación de servicio que se han sofisticado por grupos organizados como Anonymous, tras los cuales se esconde un descontento social que en conjunto, con la facilidad de colaboración que este grupo permite, deriva en nuevos vectores de ataque que también debemos tener en consideración.

Las nuevas tecnologías

Como es habitual cada vez que una tecnología va cogiendo impulso entre el gran público también nos surge un nuevo foco de posibles ataques a escala masiva, los *smartphones*, *tablets* y la proliferación de las líneas de datos móviles pueden ser una plataforma de distribución de nuevos virus entre el gran público. En estos meses han emergido nuevas versiones de caballos de Troya pero, en ciertos círculos, existe la duda de si se están desarrollando nuevas capacidades que, aprovechando la proliferación de estos terminales, ataquen a las medidas tomadas por la industria para la prevención del fraude. En este sentido, es muy importante la labor de los SOC, que deben ser nuestros ojos y oídos en Internet y nos deben proporcionar la información de todo aquello que se mueve en el entorno 'underground' para poder reaccionar con la antelación necesaria.

En el ámbito empresarial los dispositivos móviles también pueden ser una fuente de fugas de información si los usuarios corporativos hacen uso de las capacidades de estos dispositivos entremezclando el uso personal y corporativo, en el que es muy importante tanto disponer de una política clara para la nueva tendencia, la "consumerización" o BYOD (*Bring your own device*), como bastionar correctamente los dispositivos a través de aplicaciones o servicios de MDM.

La nube y sus aaS (as a Service) también nos afectan de forma directa, ya que la subcontratación de un servicio no transfiere la responsabilidad existente en el contratante y debemos ser cautelosos en la exigencia de niveles de servicio y seguridad en aquello que pongamos en manos de nuestros *partners*. Eso sin contar que un día nos podamos despertar y ver que nuestra nube ha sido cerrada por algún servicio federal porque era usada de forma ilícita por alguno de sus clientes.

El Ciberterrorismo y el espionaje industrial

Las ya no tan nuevas normativas sobre Infraestructuras Críticas podrían ser el impulso definitivo al tratamiento de la seguridad en las grandes empresas; pero no podemos dejar de mirar de soslayo las noticias -que cada vez vemos con más frecuencia- referidas al espionaje industrial, que afecta a toda empresa competitiva independientemente de si se puede considerar infraestructura crítica. De esta forma, entidades con una gran capacidad de producción pueden acceder a secretos industriales y procesos organizativos de alto valor intelectual de empresas más pequeñas y aplicarlos para producir productos "casi iguales" pero mucho más baratos.

La necesaria formación de los usuarios

Todo esto lo debemos apuntalar teniendo en cuenta la mejorable formación en seguridad de los usuarios, a los que no podemos dejar de formar, informar y concienciar. La labor de "evangelización" que debemos seguir manteniendo en las organizaciones no se debe ver mermada en ningún caso y labores como las realizadas por INTECO hacia el gran público son de gran interés para conseguir que se mejoren los conocimientos en seguridad.

Debemos mirar al futuro con cautela y sin bajar la guardia, pero con optimismo

Es vital que seamos cautelosos y nos mantengamos alerta ante los riesgos que el actual momento económico y social nos presenta. La obtención de beneficios rápidos por la industria del *malware* o la protesta social pueden convertirnos en el próximo objetivo.

Ahora bien, los recursos disponibles, bien gestionados por personas cualificadas como las que existen en las empresas, junto a socios de confianza, son garantía suficiente para mirar al futuro con optimismo, que falta nos hace estos días. ■

Raúl Amigorena
Responsable de Seguridad. Tecnología.

BANCA CÍVICA