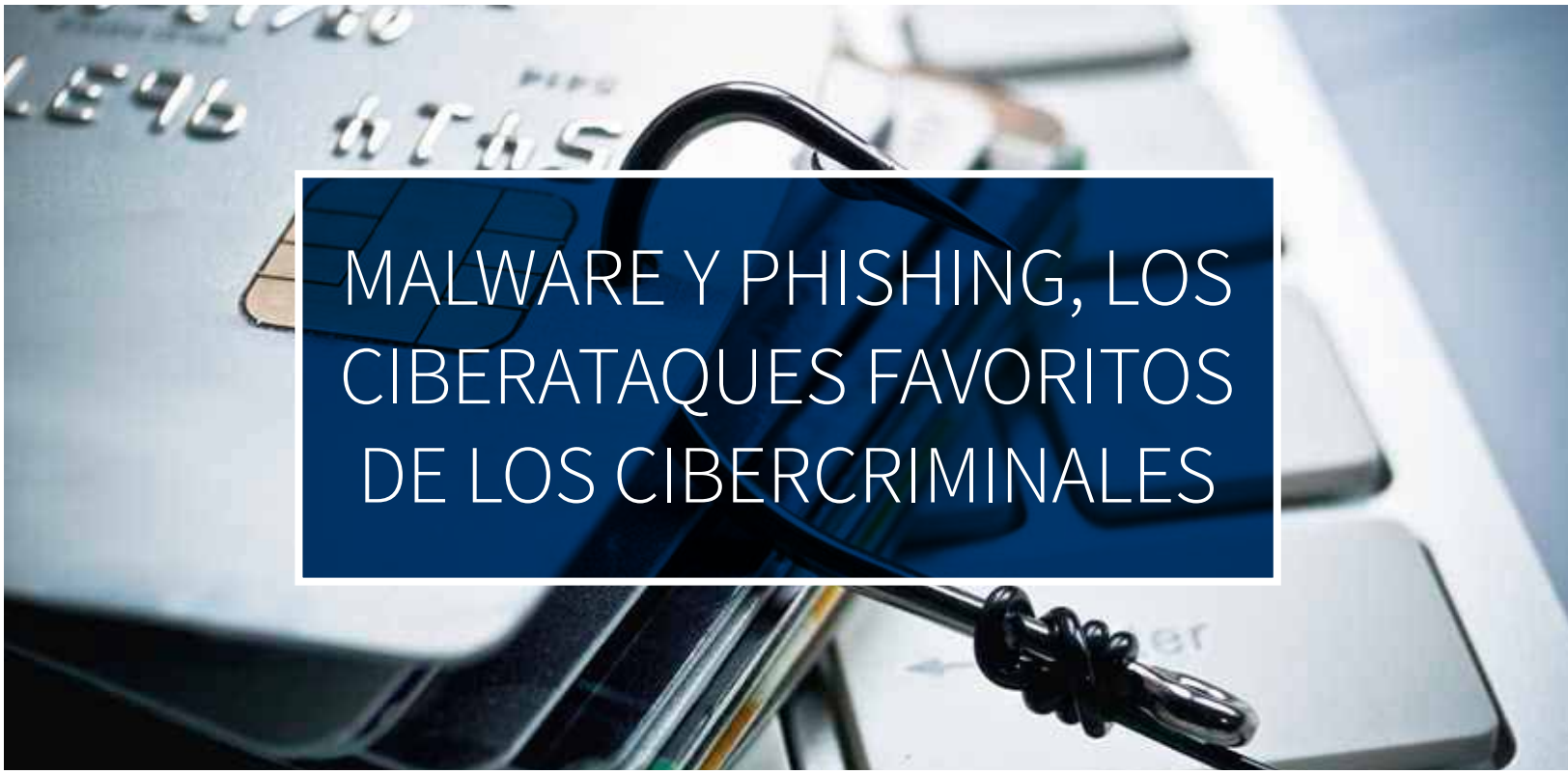
Managed secure IT | no matter what



MALWARE Y PHISHING, LOS CIBERATAQUES FAVORITOS DE LOS CIBERCRIMINALES

De acuerdo a un sondeo reciente de seguridad digital en las empresas, Estados Unidos y Canadá son los países en donde más en serio se toma el tema de las amenazas cibernéticos, desafortunadamente, esto no sucede así en América Latina.

Ese mismo documento indica que en México, solo el 15% de las empresas espera ser víctima de un ataque cibernético en los próximos dos años, lo que revela que aún faltan regulaciones y preparación para afrontar este tipo de eventos tan disruptivos.

Security

Actualmente se cree que sufrir un ataque cibernético como empresa es algo lejano o improbable; pero si algo nos enseñan los estudios recientes y la historia, es que ser víctima de los cibercriminales afecta a un negocio a una escala nunca antes vista.

El Informe sobre Amenazas para la Seguridad en Internet (ISTR), del año pasado, nos dice que el malware es una de las técnicas de infección más devastadoras y comunes en los ataques diseñados para paralizar las operaciones de una empresa y secuestrar su información.

Dicho análisis también ve una tendencia creciente, la de la minería de criptomonedas, que es cuando se instala un software apócrifo dentro de una página web para, a través de la actividad de sus usuarios, ir creando partes de una criptomoneda que, al cabo del tiempo y dependiendo qué tantas solicitudes de acceso maneja un portal, se fabrique artificialmente una unidad con valor de hasta 10 mil dólares.

Como Gerente de TI, necesitas saber que las probabilidades de ser atacado por cibercriminales es alta, pero también es necesario saber cuáles son las herramientas más usadas para poner de rodillas a un negocio de cualquier tamaño y giro.

El ISTR indica que la minería de criptomonedas tiene 8,500% de probabilidades de infectar el código fuente de tus portales web sin que te des cuenta.

Hay un 88% de posibilidades de sufrir ataques con variantes de malware que cambian de acuerdo al país o región en las que se desarrollan.

Existen 40% de probabilidades de ser vulnerado por ransomware, que secuestra bases de datos y sistemas a cambio del pago de un rescate en criptomonedas; y 46 por ciento de posibilidades de sufrir ataques por medio de variantes de ransomware y macro o script downloaders (92%).

Cualquiera de estos ataques representa grandes consecuencias para las organizaciones pues inhiben el flujo constante de ingresos, hacen que se pierda la confianza en una organización y se convierten en pérdidas masivas de capital, ya sea en la búsqueda de medidas de reacción inmediata que no se tenían previstas o en el pago de un rescate de la data secuestrada o corrupta.

El phishing también es una técnica con tendencias al crecimiento y si no se atiende, la información confidencial de socios, clientes y empleados, podría caer en manos equivocadas, representando pérdidas millonarias, sin mencionar la destrucción del prestigio y la confianza depositadas en una empresa.

Se estima que el número de URLs relacionado a las actividades de phishing, la obtención ilegal de información de datos sensibles a través del fraude cibernético, aumentó casi 183%, porcentaje del que se desprenden delitos como la malversación de activos y extorsión.

Security

Al menos un 25% de las empresas encuestadas, reportaron la interrupción de procesos de negocios que, dependiendo de la organización afectada, pueden representar miles o millones de dólares solo en pérdidas.

El 71% de los grupos de cibercriminales siguen usando correos electrónicos del tipo spear phishing para recolectar datos sensibles, lo que significa que, si bien los hackers se sofistican cada vez más en sus métodos de infección y ataque, la mayoría sigue usando los mismos métodos de siempre para atacar a sus víctimas.

Por ello, hace falta obtener nuevas regulaciones que ayuden a controlar la actividad ilícita en internet, así como adoptar métodos de prevención, monitoreo y reacción ante amenazas cibernéticas.

Los expertos recomiendan buscar la orientación de un proveedor externo de seguridad cibernética que use las herramientas más novedosas y efectivas para crear un blindaje que evite que tu negocio sea una víctima más del phishing y del malware.

El precio de un proveedor externo es mucho menor al de tener a un grupo de expertos en TI trabajando en una oficina de lunes a viernes, de las 8 de la mañana a las 5 de la tarde, dejando un hueco de al menos 15 horas sin vigilancia cibernética entre el fin de un turno y el principio de otro, ya que un proveedor externo cuenta con herramientas automatizadas que vigilan tus assets las 24 horas del día, los 365 días del año, de manera efectiva e integral.

Acércate a los expertos de Servicios Administrativos Mexis para crear un plan de protección a la medida de tus necesidades, ya que no atender el tema de la seguridad, es arriesgarse a perderlo todo en cuestión de segundos.

Las amenazas digitales no desaparecerán nunca, pero lo que puede hacerse es prepararse de la mejor manera para afrontarlas sin perder un solo segundo de productividad.

Síguenos en nuestras redes sociales:

MexisMX

Servicios Administrados Mexis, S.A. de C.V.

Mexis TI

Servicios Administrados Mexis, S.A. de C.V.