Publicado en Madrid el 29/11/2021

Tendencias en ciberdelincuencia para 2022

España es, actualmente, el tercer país más atacado de Europa por la ciberdelincuencia, con 40.000 casos de media al día. José María González, fundador de la consultora tecnológica JMG Virtual Consulting, opina que "para 2022, la sofisticación y la escala de los ciberataques seguirán batiendo récords. Aumentarán secuestros informáticos y ataques móviles. Las empresas deberán ser proactivas para prevenir estos riesgos"

Cuando en marzo de 2020 la pandemia de coronavirus confinó al mundo, muchas empresas decidieron apostar por el teletrabajo como vía para que sus trabajadores pudieran continuar con sus tareas on line. Este modelo de trabajo (una total novedad para la inmensa mayoría) descubrió ventajas: para empresas y trabajadores más posibilidades de conciliar, mejor, la vida personal y laboral; ahorro de tiempo y dinero; aumento, en muchos casos, de la productividad… Dos años y medio después parece claro que el teletrabajo ha llegado para quedarse. Ante esta nueva realidad, muchas empresas se han encontrado con que ni siquiera tienen implementadas herramientas básicas de protección del acceso remoto (autentificación de dos pasos; conexión VPN; capacitaciones de ciberseguridad para sus trabajadores, etc.)

José María González, fundador de la consultora tecnológica JMG Virtual Consulting, tiene una opinión bien formada sobre el teletrabajo. No en vano, en su empresa llevan 10 años teletrabajando desde sus sedes de Madrid, Dublín, Cádiz, Barcelona y Zaragoza “pasamos mucho tiempo fuera de nuestras oficinas, trabajando para los clientes. Sin embargo, reconozco que esto no es lo normal. Ante la nueva coyuntura impuesta por el teletrabajo, aún son pocas las empresas que saben el impacto que la ciberdelincuencia puede tener sobre este modelo híbrido. Además, a vulnerabilidades como contraseñas débiles y sistemas con errores de configuración, hay que sumar la aparición de contextos que no antes no existían y que los ciberdelincuentes tratarán de aprovechar. Por ejemplo, trabajadores que trabajan desde lugares públicos, utilizando redes abiertas e inseguras”. Según un reciente informe de Accenture, las pérdidas ocasionadas por los ciberataques durante los próximos cinco años, a nivel mundial, alcanzarán los 5 trillones de dólares. Y eso sin contar el daño reputacional.

De los noventa a 2022, cambio total de tendencias

Jordi Serra es profesor de Informática de la Universitat Oberta de Catalunya, además de experto en seguridad informática y de redes, hacking, vulnerabilidades y software. Serra analiza cual ha sido la evolución de los ciberataques desde la década del noventa, cuando se detectaron los primeros casos, a lo que se espera para 2022 “los primeros ciberataques que se hicieron, en los años 90, no tenían una motivación económica detrás. Era sólo una cuestión de ego, de tener el poder de conseguir datos que nadie más podía saber que la propia empresa o institución. Ahora el objetivo es, claramente, el dinero. Existen grupos organizados de ciberdelincuentes que buscan, exclusivamente, sacar un rédito económico. Normalmente lo hacen a través de secuestros de datos, para después pedir un rescate”. El profesor Serra habla del ransomware, una de las prácticas más habituales entre los ciberdelincuentes y que continuará siendo tendencia en 2022… aunque no será la única. El fundador de JMG Virtual Consulting detalla otras:

Campañas de desinformación y fake news. La ciberdelincuencia seguirá aprovechando la generación

de noticias falsas para desarrollar sus estrategias de phishing y estafas.

III Guerra Mundial. El próximo gran conflicto global tendrá lugar en el ciberespacio. En 2022 los ciberataques, a nivel mundial y con el objetivo de desestabilizar actividades a nivel mundial, aumentarán.

Contra la cadena de suministro. Los ataques a la cadena global de suministros también serán tendencia para el año próximo.

Filtración de datos. Principalmente dirigidos contra gobiernos y grandes empresas, cada vez serán más frecuentes y de un mayor impacto.

Contra los dispositivos móviles. Estos equipamientos se utilizan cada vez más y la ciberdelincuencia lo sabe. Especial atención a los modos de pago a través del móvil.

Criptodivisas. El dinero se está convirtiendo en software. Los ciberataques robarán y manipularán bitcoins y altcoins.

Tecnología deepfake. Vídeos y audios falsos se convertirán en un arma que se empleará en la manipulación de opiniones o cotizaciones bursátiles, así como en la obtención de permisos para acceder a datos sensibles.

Los cibercriminales aprovecharán el machine learning. El software de 'IA' está a disposición de todo el mundo. Los ciberataques lo utilizan –y utilizarán -, por ejemplo, para identificar a sus víctimas y decidir en qué momento deben atacarlas. Se emplearán herramientas de Deep Fakes para suplantar la identidad de un trabajador o imitar la voz de un directivo.

Vulnerabilidades de herramientas de comunicación. Cada vez más, se utilizan aplicaciones para comunicarse y acceder a la información. Durante la pandemia, se descubrieron importantes vulnerabilidades en servicios de VPN, plataformas como Zoom y otras aplicaciones que se ofrecen como software como servicio (SaaS, por sus siglas en inglés). Para el próximo año seguirán aumentando las posibilidades de que los ciberatacantes tomen el control de manera remota, de los dispositivos de los usuarios.

Datos de contacto:
Pepe Varela
659 277 275

Nota de prensa publicada en: Madrid

Categorías: Nacional Internet Digital Seguridad Recursos humanos/empresa