N-economía Síntesis de documentos

ENERO 2022

AUTOR: ANA LÓPEZ POLINARIO

Nº 394

FICHA TÉCNICA

Título: Ciberamenazas y Tendencias. Edición 2021

Año: 2021

Fuente: Centro Criptológico Nacional

Nº de páginas: 68

Acceso/coste: Gratuito

Localización: Disponible en el siguiente link

CONCLUSIÓN PRINCIPAL

La pandemia de la Covid-19 ha acelerado el proceso de digitalización de muchos servicios y la generalización del teletrabajo. Ello ha planteado importantes retos y desafíos, sobre todo en torno a la ciberseguridad, pues uno de los efectos inmediatos provocado por la mayor digitalización ha sido el incremento de los ciberataques. Ejemplo de ello ha sido la virulenta y cuantiosa campaña de ataques informáticos contra el sector farmacéutico para acceder a información confidencial y datos relevantes sobre las vacunas antes de su puesta en marcha. Asimismo, el interés generado entre la ciudadanía ha inundado los temas de conversación en llamadas y mensajes, hecho que los ciberdelincuentes han aprovechado, utilizando el Coronavirus como señuelo para lanzar ataques de *spear phishing*. Es lo que en el informe se ha dado en llamar "ciberpandemia".

Las entidades y organismos públicos también han sido otro de los objetivos de los ciberamenazas. Según este estudio, el 90% de los ataques se han dirigido a estos.

En cuanto al teletrabajo, los ciberdelincuentes aprovechan la fragilidad de las redes domésticas y dispositivos personales para acceder a los sistemas de información corporativos. Lo que ha puesto de manifiesto la vulnerabilidad de muchas empresas. Consecuentemente, surge la apremiante necesidad de proteger los equipos digitales y promover la formación profesional en ciberseguridad para mitigar el riesgo de esos ataques cibernéticos.

Este estudio puede resultar de gran utilidad para conocer el estado de la ciberseguridad, constituyendo un estándar de seguridad informática que permite obtener una referencia externa para empresas y organismos que deseen redefinir una estrategia de seguridad.

AUTORÍA

El informe "Ciberamenazas y Tendencias. Edición 2021" ha sido elaborado por el Centro Criptológico Nacional (CCN), un organismo del Estado español adscrito al Centro Nacional de Inteligencia, que se encarga, entre otras muchas funciones, de la elaboración y la difusión de normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas TIC del Estado y proteger la información clasificada del mismo.

El CCN integra el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las TI y el Centro Criptológico Nacional Computer Emergency Response Team (CNN-CERT).

DESCRIPCIÓN Y CONTENIDO

El documento recopila y analiza, detalladamente, los principales incidentes de ciberespionaje, amenazas, vulnerabilidades y métodos de ciberataque acontecidos en 2020 y 2021. Tales como la difusión de *fake news*, campañas de *phishing* y *ransomware*, o robo de información, como consecuencia de los cambios disruptivos y la forzosa digitalización, a nivel laboral, educativo y en la forma de comunicarse, que ha supuesto la pandemia del Coronavirus en el mundo.

Asimismo, en el informe se desvelan las tendencias que han marcado el año 2021, en términos de ciberseguridad y se proporcionan sugerencias para reducir el peligro y el impacto de las ciberamenazas.

ESTRUCTURA DEL INFORME

1. **Resumen ejecutivo**
2. **Sobre CCN-CERT, CERT Gubernamental Nacional**
3. **Vistazo 2020: ataque a la normalidad**
4. **Agentes de la amenaza**
5. **Incidentes 2020**
6. **Métodos de ataque**
7. **Que esperar en 2021**
8. **Conclusiones**

OTRAS CONCLUSIONES

El informe pone de manifiesto cómo **la Covid-19 ha sido un catalizador para la transformación digital**, lo cual ha favorecido la **hiperconectividad y la movilidad en el ciberespacio casi las 24 horas del día**, tanto en el ámbito profesional, como en el personal. **Como consecuencia, se han incrementado los factores de riesgo, en materia de ciberseguridad**, de usuarios, empresas y otras instituciones, tales como: el teletrabajo, el mayor uso de dispositios móviles conectados o la ciberpandemia (ciberataques mediante el uso del Coronavirus como cebo).

Los principales agentes o sectores que han sido **objeto de ciberataque** durante 2020 fueron: **gobiernos, Ministerios de Defensa, la industria armamentística, el sector farmacéutico, centros de investigación, las TIC, la industria de la energía, las telecomunicaciones, el sector financiero y el comercio internacional**.

El método de **ataque favorito de los ciberdelincuentes fue el *ransomware*** (secuestro de información), **seguido del *phishing* corporativo, del *malware* y del ciberespionaje y el principal objetivo ha sido el robo de información de la vacuna contra la Covid**. Cabe destacar, que no solo **se ha incrementado el número de ataques,** sino **también la cantidad de organizaciones afectadas**. Otro tipo de ataque que ha ganado gran protagonismo es el llamado ***hacktivismo***, que **utiliza canales como Twitter para difundir información y propaganda de distintos movimientos**, como Black Lives Matter, desencadenado por la muerte de George Floyd, que propició la publicación de un vídeo de **Anonymous** en el que advertían que hackearían a los departamentos de policía de EEUU.

En España, **en el año 2020, los ciberincidentes** detectados por el CCN-CERT, prácticamente **duplicaron los cometidos en 2019,** pasando de 43.000 incidentes a 82.530. De los cuales, **los catalogados de peligrosidad muy elevada, también se han doblado en 2020,** pasando de 3.172 incidentes a **7.000**.

El informe señala que **la pandemia seguirá marcando los riesgos y amenazas cibernéticas** a las que se enfrentarán empresas, entidades públicas y particulares. La especialización de los ciberdelincuentes y un entorno económico y social cada vez más cambiante, plantean **importantes retos para los profesionales de la ciberseguridad**.