CIBERSEGURIDAD

Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas

Normativas

España

Esquema Nacional de Seguridad

Estrategia Nacional de Ciberseguridad

Medidas

Actualizaciones

Gestión de riesgos de terceros

Plan de respuesta a incidentes de seguridad

Continuidad de negocio

Plan de Contingencia

Control de acceso

Copias de seguridad

Gestión de soportes

Información en circulación

Política de seguridad y normativa

Protección antimalware

Registro de actividad

Seguridad en la red

Ciber resiliencia

Plan de concienciación

Selección y evaluación de proveedores

Responsable de Seguridad de la Información (CISO)

Privacidad por diseño

Seguridad por diseño

Seguridad de endpoints

Evaluación de impacto en la privacidad (PIA)

Seguridad BYOD

Plan de Ciberseguridad o Plan Director de Seguridad

Sistema de Gestión de Seguridad de la Información

ISO 27001

COBIT

Procesos y marcos de ITIL

ISO 27701

Relacionadas

Ley de Ciberseguridad 5G

ISO 22301

Ley de Protección de Datos

ISO/IEC 27037

Ley de seguridad de las redes y sistemas de información

Reglamento de Seguridad de las Redes y Sistemas de Información (NIS)

Ayudas a la digitalización de Pymes, guía completa sobre el Kit Digital

Organismos

INCIBE

CCN-CERT

CNPIC

Guardia Civil

Policía Nacional

EMAD

AEPD

BCSC – Pais Vasco

Cataluña

Ciber.gal – Galicia

Cedid – Alicante

Oficina de Seguridad del Internauta (OSI)

Internet segura For Kids

Centro Nacional de Excelencia en Ciberseguridad

Centro de Seguridad TIC de la Comunidad Valenciana

Europa

Organismos

Centro de Competencias y Red de Ciberseguridad (ECCC)

Women4Cyber

Regulaciones

Directiva NIS

ENISA

Ley de Servicios Digitales

Ley de Mercados Digitales (DMA)

Reglamento Europeo de Ciberseguridad

RGPD

Ley de Gobierno de Datos de la UE

Europrivacy

Grecia

Irlanda

Suecia

Estonia

Chipre

Bélgica

Malta

Alemania

Polonia

Reino Unido

Francia

Austria

Italia

Dinamarca

China

EEUU

Rusia

Latinoamérica

México

Brasil

Argentina

Bolivia

Consejos y guías

Familias y usuarios principiantes

Pago seguro en Internet

Estándar PCI DSS para pagos seguros con tarjeta

Juegos

Autónomos, pymes y por sectores

Sanidad

Farmacéuticas

Videojuegos

Hoteles

Educación a distancia

Cuerpos y Fuerzas de seguridad

Comercio electrónico

Abogados

Entidades financieras

Sector energético

Sector público

Sector del transporte y logístico

Empleados

Teletrabajo

Industrial

Automóviles

Prevención / protección

Contraseñas

Revisión WIFI

Correos electrónicos

Protocolo SSH

Mitigación de ataques basados en SSH: mejores prácticas de seguridad

Seguridad reactiva frente a proactiva: ¿cuál es mejor?

Guía sobre Certificados SSL

Estafas de PayPal

Pila de seguridad

DNSSEC

¿Qué es un centro de operaciones de seguridad (SOC)?

Verificación de la identidad en las comunicaciones

Tecnología Sandboxing

Bases de datos

Alta disponibilidad

Servidor FTP

Cyber Kill Chain

Inteligencia de código abierto

Servidor proxy

Acceso remoto seguro

TeamViewer seguridad

VPN

Zero Trust

Prevención de pérdida de datos

Higiene cibernética

HSTS (HTTP Strict Transport Security)

Ciberresiliencia

Protocolo TCP/IP

Esteganografía

Desarrollo seguro

OWASP – Seguridad en la web

¿Qué es OSSTMM? Definición, historia y características

Nuevas tecnologías

Machine Learning

Procesamiento del lenguaje natural (PNL)

Redes 5G

Biometría

Computación cuántica

Piratería cuántica versus criptografía cuántica

Inteligencia artificial

Analítica aumentada

Redes neuronales artificiales

Tecnología Blue Brain

Software de inteligencia artificial

Blockchain

Máquinas virtuales

Minería de datos

Data Science

Cloud Computing

Amenazas de seguridad en la nube

Owncloud vs. Nextcloud

iPaaS

Robótica

Cobots

Nanobots

Tipos de robots

Smart cities

Big Data

Reconocimiento facial

Criptomoneda

¿Qué es Dogecoin?

Billeteras de criptomonedas

Tokens no fungibles (NFT)

Dispositivos IoT

Shodan, el Google de los dispositivos de IoT

Realidad virtual

Identidad digital

Data Fabric

Recursos

Glosario de ciberseguridad

Transformación disruptiva: ciberseguridad en la era pandémica

El navegador web más seguro de 2021

Intercambio de claves Diffie-Hellman

¿Qué es Shadow IT?

Todo lo que debes saber sobre las Ciberestafas

¿Qué son los datos psicográficos y para qué se usan?

Entendiendo la psique de un hacker moderno

Guia para ser una mujer líder en el mundo de la ciberseguridad

Web scraping

Análisis de datos

Analítica empresarial

Superficie de ataque

Seguridad de SaaS

Regtech

Códigos QR

Teléfonos móviles más seguros

Proxies residenciales

Infraestructura de escritorio virtual

Dark Web

Navegador Tor

Videollamadas

Servicios y soluciones

Control de acceso basado en roles

Herramientas

Procesamiento de eventos complejos

Técnicas de piratería de Google – Top Google Dorks

La guía completa de DevOps

Escaneo de Internet

Software

Software de trabajo remoto

UEBA: Guía completa

NetWitness

Morpheus – Nvidia

Privacy Badger

Las mejores soluciones de software de cifrado de correo electrónico

Software de Gestión de parches

Escáneres de vulnerabilidades

Soluciones de seguridad de terminales

Software de inicio de sesión único

CyberBattleSim (ciberataques)

Nikto

FireEye

JARM: herramienta de huellas digitales

Inteligencia de código abierto (OSINT)

Firma digital

Certificaciones de Ciberseguridad para empresas

Pruebas de penetración

Equipo púrpura

Cybersecurity Red Team versus Blue Team

Marco MITRE ATT&CK

Detección y respuesta extendidas (XDR)

Análisis de vulnerabilidades

Pruebas de penetración vs equipo rojo (Red Team)

Antivirus

Firewall

¿Qué es un firewall NAT y cómo funciona?

Filtrado SPF

Clasificaciones de seguridad

¿Qué es ITSM?

Cuestionario SIG

Backup

Implementar un ERP

Pruebas de software

Honeypots

Auditorías y análisis de redes e infraestructuras

Orquestación de seguridad

Sistema de detección de intrusos (IDS)

Métricas de seguridad

Métricas de ciberseguridad y KPI

Monitorización continua

Seguridad perimetral

Modelado de amenazas

Test de intrusión

¿Qué son algoritmos de cifrado? Tipos y características

Monitorización en la nube

Caza de ciberamenazas

Otros servicios

Ethical Hacking

Análisis forense

Software

Evidencia digital

Análisis forense en dispositivos móviles

Ciberseguros

Perito informático

Abogados

Formación

Full Stack Developer

Amenazas y vulnerabilidades

Ransomware

Ryuk

Jokeroo

Netwalker

Egregor

Zeppelin

Aumento de privilegios

Spoofing

Suplantación de identidad

Hacktivismo

Ataques de kerberoasting

Banner Grabbing

Amenaza persistente avanzada (APT)

Minería de criptomonedas – Cryptohacking

Malvertising

Drive by Downloads

Firma de archivo de malware

Island Hopping

Amenazas móviles

BadPower

Robo de datos

Phishing

Ejecución remota de código (troyano) – Remote Access Trojan (RAT)

Distributed Denial of Service (DDoS)

Ataques de Denegación de servicio de rescate (RDoS)

Secuestro de DLL

DNS Hijacking

Ataque de relleno de credenciales

Malware

Trickbot

Emotet, ¿qué es y cómo funciona?

Koobface

Dridex

Trojan Glupteba

Grooming

Ciberacoso

Cybersquatting y Typosquatting

Fraude bancario

Formjacking

Ciberespionaje

Exploits

SIM Swapping

Footprinting y Fingerprinting

Bootnets

Wiper (limpiaparabrisas)

Física

Tailgating y Piggybacking

Ingeniería social inversa

Shoulder Surfing

Dumpster Diving

Vulnerabilidades

Desbordamiento de buffer

Condición de carrera

Error de formato de cadena

Cross Site Scripting

Inyección SQL

Ciberataques

España

Los 15 ciberataques más importantes en 2021

Empresas

España

Madrid

Barcelona

Valencia

País Vasco

Andalucía

Navarra

Asturias

Galicia

Zaragoza

Santander

La Rioja

Castilla – León

Extremadura

Murcia

Castilla La Mancha

Mallorca

Canarias

EE.UU.

China

Rusia

India

Canadá

Europa

Alemania

Francia

Reino Unido

Italia

Portugal

Bélgica

Irlanda

Noruega

Latinoamérica

México

Colombia

Brasil

Argentina

Chile

Venezuela

Perú

Ecuador

Uruguay

Formación

Libros

Cursos

Máster

Certificaciones

Empleo

Tendencias en Ciberseguridad

La ciberseguridad en 2021

Previsiones de ciberseguridad y privacidad de datos 2022

ENTRADAS

PUBLICADO ELOCTUBRE 16, 2023

¿Conoces el nivel de ciberRiesgo de tus empleados en la Era Digital?

zepo ciberseguridad empresas

En la era digital actual, la tecnología ha cambiado drásticamente la forma en que las empresas operan y se comunican. Sin embargo, esta revolución también ha traído consigo un oscuro y persistente desafío: los ciberataques. En un mundo cada vez más conectado, las amenazas cibernéticas se han convertido en una realidad omnipresente que afecta a empresas de todos los tamaños y sectores. En este contexto, surge la necesidad de fortalecer las defensas empresariales y reconocer la importancia de las personas en la ecuación de la ciberseguridad.

Los desafíos de la ciberseguridad en un mundo conectado

Los ciberataques han alcanzado un nivel de sofisticación sin precedentes. Las noticias sobre brechas de seguridad y filtraciones de datos en empresas de renombre inundan los titulares con regularidad y reflejan la magnitud de la amenaza.

Ataques de ransomware que paralizan operaciones, robos de información confidencial o estafas de phishing cada vez más convincentes son solo algunos de los múltiples ejemplos que se dan. La concienciación en ciberseguridad de las empresas se vuelve fundamental para proteger los activos digitales y salvaguardar la confianza de los clientes.

Estos ataques no solo tienen consecuencias económicas, sino que también pueden atacar la reputación de una organización y dañar su posición en el mercado. Es fundamental que los líderes empresariales comprendan que la ciberseguridad ya no es un aspecto secundario o un problema puntual, sino un asunto estratégico que requiere atención y acción en todos los niveles de la organización.

Vulnerabilidad Humana: El empleado, el eslabón más débil de la cadena

A pesar de la inversión en tecnologías avanzadas de seguridad, los ciberdelincuentes siguen encontrando formas de saltar todos los mecanismos de defensa que las organizaciones utilizan en el mundo digital.

Uno de los puntos más débiles en temas de seguridad cibernética es el factor humano. Los ataques de ingeniería social dirigidos a las personas continúan siendo una táctica efectiva para los ciberdelincuentes (más del 90% de los ciberataques comienzan con un fallo humano).

A menudo, son los propios empleados quienes se convierten en la puerta de entrada involuntaria para los ciberdelincuentes. La falta de formación y concienciación en ciberseguridad puede llevar a errores costosos, como descargar archivos maliciosos o proporcionar información confidencial.

La educación en ciberseguridad debe ser una prioridad para todas las empresas. El empoderamiento de los empleados es clave para la construcción de un firewall humano que sea capaz de identificar y reportar posibles amenazas para así marcar la diferencia a la hora de crear una defensa sólida ante los ciberataques.

Creando una cultura de ciberseguridad en la organización

Una prevención efectiva de ciberataques no solo se consigue con medios tecnológicos, sino que requiere crear y fomentar una cultura de ciberseguridad en la organización.

Un requisito fundamental es que las empresas inviertan en programas de simulación y formación en ciberseguridad que faciliten la tarea de abordar diferentes problemáticas relacionadas con las vulnerabilidades informáticas y que permitan una segmentación muy específica entre los distintos tipos de empleados, personalizando al máximo sus competencias según el área o campo al que pertenezcan. La concienciación en ciberseguridad no debe ser un evento único, sino un proceso continuo de aprendizaje para mantenerse al día con las últimas amenazas y tendencias, aprovechando metodologías como el Learning by Doing.

Además, es esencial fomentar un clima de transparencia en el que el empleado se sienta seguro al informar acerca de incidentes o sospechas de ciberataques. La colaboración entre departamentos y la implementación de políticas de seguridad cibernética eficaces pueden contribuir a un entorno empresarial más resistente a las amenazas digitales para asegurar el bienestar cibernético de los empleados.

Zepo: La solución integral para la ciberseguridad empresarial

En este desafiante escenario, podemos destacar a Zepo como una herramienta líder en ciberseguridad para empresas. Zepo, creada por profesionales de la educación y desarrollada por expertos en ciberseguridad, es una plataforma intuitiva y fácil de usar que permite lanzar simulaciones de ciberataques automatizados y personalizables, de forma que las empresas puedan poner a prueba la preparación de sus empleados frente a ciberataques.

Automatiza la creación de escenarios de ingeniería social de forma sencilla

Zepo ofrece escenarios de ingeniería social altamente personalizados en función del tipo de organización y de las necesidades de cada empleado. Esta simulación ayuda a las empresas a identificar áreas de mejora y a fortalecer las defensas contra los ataques reales. Además, permite exponer a los empleados ante situaciones reales simuladas para aprender a gestionarlas.

Forma a tus empleados

La plataforma de Zepo automatiza el proceso de formación gracias a una tecnología propia que permite ofrecer cursos adaptados a las necesidades de cada empleado. De esta manera, los empleados pueden adquirir los conocimientos necesarios en ciberseguridad de una manera amena y efectiva.

Monitoriza el progreso de tu organización

Con Zepo, las empresas pueden obtener una visión real del nivel de vulnerabilidad tanto a nivel de organización, como de departamento y de empleado. Esto permite tomar decisiones objetivas basadas en datos reales de la organización para mejorar la seguridad en áreas específicas. Además, Zepo permite gestionar de forma automática el proceso de control de seguimiento y cumplimiento de la formación.

En resumen, la creciente ola de ciberataques a nivel mundial supone una llamada de atención para las empresas. La ciberseguridad ya no puede ser subestimada ni delegada únicamente a equipos de tecnología.

Reconocer a las personas como el eslabón más débil en esta cadena y comprometerse a educar y concienciar a los empleados son pasos cruciales para mitigar los riesgos y fortalecer las defensas cibernéticas de las organizaciones en un mundo digital cada vez más peligroso. Esto contribuirá positivamente a fomentar el bienestar cibernético de los empleados y de las empresas.

PUBLICADO ELAGOSTO 8, 2023

5 razones para estudiar un máster en ciberseguridad online

razones para estudiar máster de ciberseguridad online

La ciberseguridad es cada vez más relevante para empresas, instituciones y organismos públicos y usuarios particulares. Con una demanda cada vez mayor de perfiles profesionales especializados en la materia, estudiar un máster en ciberseguridad online es una de las mejores formas de especializarse en un ámbito con una amplia variedad de salidas profesionales.

¿Por qué estudiar un máster en ciberseguridad online en la Universidad Isabel I?

En la actualidad, ninguna entidad está exenta de sufrir un ciberataque o incidente de seguridad, eventos cuyas consecuencias para las organizaciones son tanto económicas (costes derivados de sanciones y de los daños sufridos) como reputacionales (pérdida de confianza de clientes y usuarios). Prevenir estos incidentes se ha convertido en un elemento clave para muchas empresas y organizaciones, lo que ha convertido a la ciberseguridad en una necesidad ineludible para ellas.

Esto a su vez ha hecho que los perfiles profesionales especializados en esta materia sean cada vez más demandados y que hayan aumentado considerablemente el número de salidas profesionales en ciberseguridad. Pero las salidas profesionales son solo una de las cinco razones de por qué estudiar ciberseguridad a través de un máster online es una de las mejores opciones para tu desarrollo y crecimiento profesional.

Aparte de poder estudiar desde casa, el máster de ciberseguridad online ofrece una formación en ciberseguridad completa y práctica, con la que obtendrás los conocimientos necesarios para desempeñar una profesión que no deja de crecer día a día para poder hacer frente a todo tipo de ciberamenazas y conseguir el objetivo principal de mantener la integridad, confidencialidad y disponibilidad de la información, algo que no solo es muy necesario, sino también imprescindible tanto en grandes empresas como en pymes.

Mayor especialización

El máster en ciberseguridad online está pensado para estudiantes de informática y otras formaciones profesionales relacionadas, así como para personas con conocimientos informáticos suficientes para poder realizar esta formación, que quieran especializarse en seguridad de la información y poder poner sus conocimientos y experiencia al servicio de cualquier tipo de organización pública o privada o de usuarios particulares, para prevenir ciberataques y robos o pérdidas de información confidencial, así como daños a equipos, dispositivos e infraestructuras informáticas.

Gracias a la formación específica impartida en el máster en ciberseguridad online, obtendrás conocimientos y capacidades específicas en ciberseguridad, completamente actualizados y con un desempeño práctico desde el principio, de manera que podrás especializarte en una de las materias más demandadas profesionalmente y con una gran proyección de futuro.

Desde ciberseguridad industrial a ciberseguridad móvil, pasando por biometría, criptografía, informática forense y hacking ético, con el máster en ciberseguridad online podrás prepararte para desempeñar cualquier puesto de trabajo relacionado con la seguridad de la información, la prevención, detección y mitigación de ciberamenazas y la formación y asesoramiento sobre la materia.

Perfil profesional muy demandado

Cómo decíamos, la ciberseguridad en las empresas y otras organizaciones es cada vez más importante y esencial, lo que ha convertido a los expertos en ciberseguridad en uno los perfiles profesionales cada vez más demandados, de hecho, estadísticas recientes sobre ciberseguridad nos dicen que aún se está lejos de poder cubrir todos los puestos especializados en ciberseguridad que sería necesario en empresas y organizaciones.

Por lo tanto, cursar el máster en ciberseguridad online es garantía de encontrar un puesto de trabajo con relativa facilidad una vez finalizados los estudios y las prácticas.

Diferentes salidas profesionales en ciberseguridad

Cómo decíamos, estudiar el máster en ciberseguridad online te preparará para poder optar a un amplio abanico de salidas profesionales, porque son muchos los puestos que requieren una formación específica en ciberseguridad, algunos incluso no tienen por qué ser específicamente técnicos, sino que también podrás optar a puestos donde contar con una formación especializada en ciberseguridad te hará destacar frente a otros candidatos (por ejemplo, en puestos relacionados con protección de datos, donde podrás desempeñar el puesto del delegado de protección de datos).

Así, entre las salidas profesionales que encontrarás tras cursar el máster en ciberseguridad online, tienes puestos como:

Administrador de seguridad de sistemas y redes.

Arquitecto de sistemas de seguridad.

Ingeniero de control de ciberseguridad.

Arquitecto de análisis de riesgos.

Gestor de protección de datos.

Consultor de seguridad y hacking ético.

Analista de informática forense

Perito judicial tecnológico.

Ingeniero de ventas de ciberseguridad.

Especialista en respuesta ante incidentes.

Salarios

Si bien la vocación suele ser una de las principales razones para cursar unos determinados estudios, el salario, junto a las salidas profesionales, es otra razón igual de importante.

El salario medio para los profesionales especializados en ciberseguridad en España oscila entre los 30.000 y los 60.000 anuales (dependiendo de la experiencia, la antigüedad y el cargo ocupado). Un salario muy por encima de la media salarial actual.

Amplias posibilidades de desarrollo profesional

Cursar el máster en ciberseguridad online no solo te abrirá las puertas a una amplia variedad de puestos profesionales, sino que también te permitirá desarrollar una carrera profesional con bastante proyección de futuro, no solo porque la ciberseguridad va a seguir cobrando cada vez mayor relevancia como consecuencia de un mundo cada vez más digitalizado y dependiente de internet, sino porque también es una profesión en la que podrás evolucionar y seguir avanzando y creciendo.

La escasez de expertos en ciberseguridad no solo te permite entrar con más facilidad en el mercado laboral, sino que también encontrarás grandes oportunidades para crecer dentro de las propias organizaciones; podrás empezar desde cualquier nivel y escalar puestos hasta convertirte en el CISO (director de seguridad de la información) o el RSI (responsable de seguridad de la información) de la organización o el ya mencionado delegado de protección de datos.

La importancia de la ciberseguridad

La ciberseguridad cada vez es más importante y crucial para empresas y otras organizaciones, tanto públicas como privadas, el número de ciberataques y ciberamenazas no deja de crecer y los escenarios son cada vez más complejos. Formarse en ciberseguridad a través del máster en ciberseguridad online es la mejor forma de prepararse para los retos que presenta esta materia, encontrar un empleo cualificado, altamente demandado y en el que podrás desarrollar tu carrera profesional.

Cualquier empresa que quiera evitar las pérdidas y costes derivados de sufrir un incidente de seguridad, sea este involuntario o causado por un ciberataque, debe contar con un profesional especializado en ciberseguridad en su plantilla o contratar los servicios de un consultor externo, ya que es la mejor forma de prevenir y evitar problemas graves relacionados con la seguridad de la información. Y esto es algo que en el futuro irá a más; la ciberseguridad es algo que las empresas ya no pueden ignorar.

Por lo que, en conclusión, la pregunta no es por qué estudiar ciberseguridad, sino por qué no formarte en una profesión con un futuro prometedor gracias al máster en ciberseguridad online.

PUBLICADO ELFEBRERO 4, 2022

Los ciberdelitos no dejan de aumentar

aumento de los ciberdelitos

El desarrollo de internet ha ofrecido innumerables ventajas a la humanidad, pero también ciertos riesgos. El entorno online ha sido el escenario propicio para la aparición de nuevos tipos de delitos que pueden suponer un enorme riesgo para los usuarios. Los ciberdelincuentes, hackers o piratas

informáticos siempre están buscando nuevas maneras de conseguir sus propósitos ilícitos, aprovechándose de la falta de conocimiento o la ingenuidad de muchos usuarios.

La mejor manera de prevenir los ciberdelitos es contar con los conocimientos y herramientas adecuadas para no caer en las trampas que ponen los ciberdelincuentes. Sin embargo, en ocasiones toda precaución es poca y nadie está libre de las garras de los piratas informáticos. Si ya has sido víctima de algún ciberdelincuente, entonces necesitas un abogado penalista.

¿Qué es un ciberdelito?

Un ciberdelito es aquel delito que es cometido por un ciberdelincuente en el espacio digital mediante el uso de métodos informáticos.

En un principio, estos ciberdelitos se basaban en la difusión de virus o malware que ocasionaban grandes perjuicios a los equipos informáticos. Sin embargo, con el paso de los años los delitos informáticos se han ido diversificando y en la actualidad pueden adoptar numerosas formas y tener intenciones muy diversas.

A las personas que realizan este tipo de delitos se les suelen llamar hackers, pero en realidad el término «hacker» no tiene por qué hacer referencia a personas relacionadas con los ciberdelitos. En realidad, sería más apropiado llamarles ciberdelincuentes o piratas informáticos.

Pero, ¿cuáles son los ciberdelitos más frecuentes hoy en día y en los que es más fácil caer?

¿Cuáles son los ciberdelitos más comunes en internet?

Uno de los grandes problemas de la seguridad informática es la gran rapidez con la que evolucionan los métodos empleados por los ciberdelincuentes. Por ello, no resulta extraño que muchos usuarios sigan cayendo en alguna de estas trampas.

Estafas y fraudes

Las estafas online están a la orden del día. Los ciberdelincuentes buscan robar las cuentas bancarias de sus víctimas o engañarles para que les paguen determinadas cantidades de dinero. A este tipo de estafas online se les suele llamar scam, y son unas de las más frecuentes en la red.

Robo y suplantación de identidad

El phishing o suplantación de identidad también es otro de los delitos que más han aumentado en los últimos años. Los ciberdelincuentes buscan conocer los datos personales o las credenciales de la víctima para hacerse pasar por ella. La suplantación de identidad es muy peligrosa ya que se suele usar con fines maliciosos, como acceder a cuentas bancarias, hacer contratos a nombre de la víctima, etc.

Revelación de secretos

Uno de los ciberdelitos de los que suelen ser víctima las empresas es la revelación de información confidencial. Los piratas informáticos se cuelan en los equipos de las empresas para conocer información secreta y revelarla a otros a cambio de dinero. Aunque son las organizaciones quienes suelen ser el objetivo de estos delitos online, las personas físicas también pueden ser víctima de los mismos, por ejemplo cuando se utiliza información personal privada para causar un perjuicio o menoscabar el honor o la intimidad de la persona.

Ciberacoso y amenazas

Con la creciente popularidad de las redes sociales han aumentado enormemente los casos de ciberacoso. Las formas que puede adoptar este tipo de delito son numerosas, siendo las más frecuentes el acoso sexual o la sextorsión. Las víctimas más habituales de este tipo de delitos en internet suelen ser menores de edad y adolescentes.

Pornografía infantil

En ocasiones, los delitos sexuales en internet pueden ir un paso más allá y llegar a la pornografía sexual, que consiste en la difusión de contenidos de índole sexual en internet, muchas veces bajo coacción o sin el conocimiento de la víctima. Esto es especialmente grave cuando se trata de menores de edad

Ataques informáticos

Virus, troyanos, ransomware, spyware, bombas lógicas, ataques de denegación de servicio, gusanos informáticos... Los ataques informáticos han adoptado numerosas formas con el avance de las tecnologías, y son cada vez más difíciles de detectar. El objetivo suele ser controlar el equipo del usuario con diferentes objetivos: robo de datos, solicitar dinero para devolver el control del equipo, o incluso «tirar» toda la infraestructura informática de la víctima.

Contra la propiedad intelectual

Por último, los delitos contra la propiedad intelectual también han aumentado mucho debido a la dificultad para rastrear este tipo de propiedades en internet. El uso o apropiación indebida de

documentos, archivos, textos, imágenes, vídeos o contenido de cualquier índole está a la orden del día y, lo peor de todo, en muchas ocasiones quedan impunes.

¿Víctima de ciberdelito? Contrata un abogado penalista

Es frecuente ver cómo las víctimas de ciberdelitos no saben qué hacer o a quién acudir. Sin embargo, la respuesta es sencilla. Los primero es acudir a la Guardia Civil o la Policía y contratar a un abogado penalista que te ayude a la hora de llevar el proceso judicial.

Los abogados penalista especialistas en ciberdelitos son la mejor opción de la hora de defender a las víctimas de este tipo de actividades malintencionadas:

Delitos contra la confidencialidad, la integridad y la disposición de los datos y sistemas informáticos: acceso ilícito a un sistema, interceptación ilícita de datos e interferencia en el funcionamiento de un sistema informático.

Delitos informáticos: falsificación informática de datos y fraude informático.

Delitos relacionados con el contenido: producción, oferta, difusión, adquisición de contenidos de pornografía infantil.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Ciberdelitos de clase 1 y 2, phishing, hacking, malware y ransomware.

Así que, si por desgracia has sido víctima de algún delito en internet, que sepas que la solución a tus problemas está al alcance de la mano y pasa por contratar a un buen abogado penalista especializado en ciberdelitos.

PUBLICADO ELDICIEMBRE 9, 2021

10 consejos para mejorar la seguridad de tu WordPress

mejorar seguridad en wordpress

¿Tienes un blog personal, una página web corporativa o una tienda online en WordPress? En ese caso, este artículo te interesa. En él te damos una serie de consejos y recomendaciones para mejorar la seguridad de tu WordPress y evitar que tu sitio web sea víctima de los ciberdelincuentes.

Los 10 mejores consejos de seguridad para WordPress

WordPress es el creador de contenido online más utilizado del mundo por su sencillez de uso y por las grandes posibilidades que ofrece gracias a su versatilidad. Aunque es una plataforma que se

actualiza constantemente e incluye cada cierto tiempo nuevos parches de seguridad, eso no quiere decir que sea una herramienta totalmente segura. Por eso, nunca está de más tomar precauciones para garantizar la seguridad en WordPress.

Elige un hosting de confianza

WordPress ofrece su propio servicio de hosting, pero si quieres elegir otra empresa para alojar tu web, has de tener en cuenta que debe ser un hosting confiable.

Existen muchos servicios de alojamiento a precios muy reducidos, pero que ofrecen servidores compartidos, de poca calidad o con nulo soporte técnico. Lo mejor es optar por un hosting de alta calidad que cuente con servidores dedicados y que ofrezca soporte de seguridad al usuario.

Otra opción es instalar WordPress en servidor local, para acostumbrarse a la interfaz y funcionalidades de la plataforma antes de poner la web online. Existen diversas herramientas para ello, como XAMPP.

Usa la verificación en dos pasos

Una de las nuevas exigencias en materia de protección de datos es usar la autenticación de dos factores. Con este nuevo método, cualquier persona que quiera acceder a tu WordPress deberá introducir su usuario y contraseña, pero además tendrá que confirmar su identidad a través de un código recibido por SMS o email.

Instala el certificado SSL

El certificado SSL o Secure Sockets Layer permite que los paquetes de datos entre la página web y el servidor viajen de manera segura. Esto es especialmente importante cuando los usuarios tengan que introducir datos personales, por ejemplo a la hora de realizar compras online.

Distinguirás a las páginas que tienen instalado este certificado porque su url empieza por https:// en lugar de http://.

Cuidado con los plugins

Los plugins de WordPress pueden llegar a ser muy útiles por las múltiples funcionalidades que pueden aportar a tu página web. Sin embargo, también hay que tener cuidado con ellos.

Saturar la página de plugins puede hacer que la web tarde mucho más en cargar, lo que repercute negativamente en su posicionamiento en Google. Por otro lado, hay que evitar descargar plugins desactualizados o de editores poco confiables y desconocidos.

Del mismo modo, revisa periódicamente los plugins que tengas instalados. Actualiza los que estén desfasados y elimina aquellos que ya no utilices.

Haz copias de seguridad

Hacer copias de seguridad es básico para garantizar que no pierdes la información en caso de que se produzca un fallo de seguridad. En este caso, no se trata de un consejo de seguridad destinado a prevenir, sino a minimizar los daños en caso de que se produzca una brecha de seguridad.

Existen proveedores de hosting que realizan copias de seguridad de forma automática, por eso ya te hemos comentado que siempre es mejor elegir un servicio de alojamiento de calidad.

Cambia la URL de inicio de sesión

Por defecto, WordPress utiliza una url de inicio de sesión como la siguiente: http: //mipaginaweb.com/wp-admin. Los atacantes suelen usar programas llamados GWDb que introducen nombres de usuario y contraseñas al azar, hasta que consiguen dar con la clave. Sin embargo, cambiando la url de inicio de sesión te proteges contra este tipo de prácticas. Para hacerlo puedes recurrir a herramientas como iThemes.

Protege el archivo wp-config.php

El archivo wp-config.php es uno de los más importantes de tu web ya que contiene la información sobre la instalación de WordPress. Para proteger este archivo simplemente has de colocarlo en un lugar jerárquico más alto en tu directorio raíz. El archivo seguirá ahí y continuará siendo funcional y visible para ti, pero no para los hackers.

Vigila permisos y credenciales de acceso

Otro de los principales consejos de seguridad para tu WordPress es utilizar contraseñas seguras que consten de una serie de caracteres alfanuméricos elegidos al azar. También hay que elegir nombres de usuario seguros, evitando el típico «Admin» o similares.

Por otro lado, hay que otorgar los permisos necesarios a cada usuario, en función de si se trata de super administradores, administradores, editores, autores, colaboradores o suscriptores.

Evita el spam

Otro consejo de seguridad para tu WordPress es filtrar los comentarios spam. Estos no solo resultan molestos y perjudiciales para el posicionamiento SEO, sino que también pueden suponer un riesgo de seguridad para los usuarios. Imagina que un usuario pincha (voluntaria o accidentalmente) en un enlace de un comentario spam que le descarga un virus en su equipo. No pensaría que tu página web es un sitio seguro, ¿verdad?

Usa herramientas anti malware

Existen numerosas herramientas anti malware o anti spyware en el mercado que permiten analizar tu página en busca de software malicioso. Es recomendable usar estas herramientas de forma periódica para comprobar que tu web está libre de virus y, en caso de que exista algún tipo de malware, poder eliminarlo a tiempo.

En definitiva, estos son algunos de los mejores consejos de seguridad para WordPress que debes poner en práctica en tu página web. No olvides que internet puede ser un lugar maravilloso pero que también esconde amenazas ocultas que pueden acarrear graves consecuencias, por lo que toda precaución siempre es poca.

PUBLICADO ELNOVIEMBRE 29, 2021

Cómo asegurar la protección de tu sitio web

consejos para proteger tu pagina web

Hoy en día crear una página web es muy sencillo y se puede hacer en cuestión de minutos. Sin embargo, todavía existen muchos usuarios que ignoran los riesgos que existen en la red y que pueden poner en peligro no solo su web, sino incluso su propia intimidad y la de sus visitantes. Por eso, en este artículo te damos una serie de recomendaciones para asegurar la protección de tu sitio web.

7 consejos para proteger tu página web

¿Te gustaría tener tu propio blog personal o una tienda online? Entonces, debes saber que existen una serie de consejos que debes llevar a cabo para tener un web seguro. No te preocupes, a continuación te damos unas pautas que debes seguir sí o sí.

Elegir un hosting confiable

Existen numerosas empresas, sobre todo extranjeras, que ofrecen servicios de alojamiento a precios muy bajos. Sin embargo, suele tratarse de hosting compartidos, de baja calidad o que ofrecen un nulo soporte a sus usuarios en caso de que se produzca una brecha de seguridad. Por eso, antes de elegir un hosting debes asegurarte de que es confiable y que tiene una probada reputación.

Usar certificado SSL

Los certificados SSL o Secure Sockets Layer permiten que la información entre la web y el servidor viaje de forma segura. Esto es fundamental a la hora de hacer transacciones de información en la red. Puedes distinguir a las webs que cuentan con estos certificados porque la dirección web empieza con https:// en vez de http://.

No usar demasiados plugins

Los plugins pueden ser muy útiles a la hora de incorporar nuevas funcionalidades a la página web. Sin embargo, también cuentan con algunos inconvenientes. Por un lado, saturar la web de plugins puede repercutir negativamente en la velocidad de carga de la página, y por ende, en su posicionamiento SEO. Además, los plugins pueden ser una puerta de entrada a virus y malware, sobre todo aquellos que están desactualizados o que provienen de editores desconocidos.

Gestionar correctamente permisos y accesos

Es imprescindible crear contraseñas de acceso fuertes y que no sean fácilmente descifrables para los atacantes. Lo mismo sucede con los nombres de usuario. Por ejemplo, hay que evitar poner como nombre de usuario «Admin» o similares. Asimismo, se deben gestionar correctamente los accesos a la web, otorgando los permisos necesarios en caso de que se trate de usuarios, editores o administradores.

Escanear la web en busca de malware

Existen diversas herramientas que permiten escanear una página web en busca de algún tipo de amenaza. Usar este tipo de software es fundamental para detectar si un atacante ha instalado algún tipo de software malicioso en nuestra web con el objetivo de robar información o de hacerse con el control de la misma.

Eliminar los comentarios spam

Los comentarios spam no solo son muy molestos, sino que pueden suponer un riesgo para la seguridad, no tanto de la propia página web, sino de los usuarios que la visitan. Imagina que un usuario pincha en un enlace spam de un comentario, que le descarga un virus en su ordenador. ¿Qué imagen daría tu página web si esto ocurriese?

Hacer copias de seguridad periódicas

Por último, no debes olvidarte de realizar copias de seguridad de tu página web cada cierto tiempo. Gracias a ello podrás tener la información a salvo en caso de que se produzca alguna brecha de seguridad. Hoy en día existen empresas con planes de hosting que realizan copias de seguridad automáticas y que incluso te avisan si se ha producido algún ataque o un acceso sospechoso.

En resumen, estas son algunas de las recomendaciones para proteger tu página web. Y recuerda, en internet toda precaución es poca.

PUBLICADO ELABRIL 15, 2021

La ciberseguridad en 2021

ciberseguridad

Gracias a los estándares tecnológicos en constante desarrollo, la ciberseguridad se ha convertido en la prioridad número uno para las empresas y las personas en todas partes. Los atacantes de la red se esfuerzan constantemente por socavar la protección de los datos personales y de la empresa, por lo que es más difícil que nunca para las personas mantenerse seguras.

El papel vital que desempeña la ciberseguridad en la protección de nuestra privacidad, derechos, libertades, incluida nuestra seguridad física, será más prominente que nunca durante 2021.

Cada vez más nuestra infraestructura vital se encuentra en línea y vulnerable a ataques digitales. Las infracciones relacionadas con la filtración de información personal son cada vez más frecuentes y más grandes, y hay una creciente conciencia de la interferencia política y los ataques cibernéticos sancionados por el estado.

La importancia de la ciberseguridad es, sin duda, una cuestión cada vez mayor de interés público.

Se están produciendo cambios con la entrada en la nueva década, y 2021 podría tener más desafíos de ciberseguridad para las empresas.

Entonces, ¿cuáles son algunas de estas amenazas cibernéticas potenciales y cómo pueden las empresas prepararse para ellas?

Tendencias en Ciberseguridad en 2021

Confiamos en la tecnología para resolver muchos de los problemas que enfrentamos, tanto a escala global como personal.

Desde teléfonos inteligentes y asistentes personales de IA hasta viajes espaciales, curar el cáncer y abordar el cambio climático. Pero a medida que el mundo se conecta cada vez más, las oportunidades para que los malos se aprovechen con fines de lucro o con fines políticos aumenta inevitablemente.

Aquí analizaremos la predicción anual de los eventos que creo impactarán el panorama de ciberseguridad en este año. Tratemos de imaginar qué amenazas y malos actores influirán en la arena cibernética en los próximos 12 meses.

1. Mayor importancia de la Inteligencia artificial (IA)

La inteligencia artificial (IA) desempeñará un papel cada vez más importante tanto en ciberataque como en defensa.

La IA es la nueva carrera armamentista, pero a diferencia de las carreras armamentistas anteriores, cualquiera puede involucrarse. No hay necesidad del tipo de recursos que anteriormente solo estaban disponibles para los gobiernos.

Esto significa que si bien la IA está siendo investigada y desarrollada, sin duda, como un medio para paralizar la infraestructura civil y de defensa de un estado enemigo durante la guerra, también es fácilmente desplegable por bandas criminales y organizaciones terroristas.

Entonces, más que entre naciones, la carrera de hoy es entre hackers, crackers, phishers y ladrones de datos, y los expertos en ciberseguridad cuyo trabajo es abordar esas amenazas antes de que nos causen daño.

Del mismo modo que la IA puede «aprender» a detectar patrones de coincidencia o comportamiento que pueden indicar un intento de ataque, también puede aprender a adaptarse para disfrazar el mismo comportamiento y atravesar nuestras defensas.

Este desarrollo paralelo de capacidades ofensivas y defensivas se convertirá en un tema cada vez más presente a medida que los sistemas de IA se vuelvan más complejos y, lo que es más importante, más disponibles y más fáciles de implementar.

Todo, desde el correo electrónico no deseado, intenta engañarnos para que revelemos los detalles de nuestra tarjeta de crédito. Hasta los ataques de denegación de servicio diseñados para deshabilitar la infraestructura crítica, crecerán en frecuencia y sofisticación.

Por otro lado, la tecnología que nos hace víctimas, como los algoritmos de seguridad de aprendizaje profundo, la automatización de sistemas que son vulnerables a errores humanos y la protección de identidad biométrica, también está progresando.

2. Incremento de divisiones políticas y económicas

Las divisiones políticas y económicas entre el este y el oeste conducen a mayores amenazas de seguridad.

Internet y el mundo en línea es una entidad internacional, relativamente libre de fronteras o restricciones a la libre circulación de información e ideas. Se construyó de esa manera porque sus arquitectos entienden la importancia de la cooperación internacional cuando se trata de acceder al talento y los recursos. Pero eso es todo solo una ilusión. Las corporaciones, redes y asociaciones que proporcionan la infraestructura detrás de escena son entidades legales obligadas a cumplir con las leyes y regulaciones nacionales.

Sin un final a la vista de la «guerra comercial» entre las superpotencias del mundo, se habla de fracturas entre organizaciones internacionales como la ONU o la UE. Y una carrera armamentista impulsada por la tecnología entre las naciones que son competidores económicos. Eso podría tener consecuencias muy aterradoras.

Hace solo unas semanas, Rusia anunció que había probado una Internet ‘desconectada’, básicamente una alternativa nacional a Internet global, que podría dar a su Gobierno el control sobre lo que los ciudadanos pueden acceder en la web. Existen países, como China e Irán, en los que ya se censura el contenido y se obstruye el acceso a información externa.

En 2019, también vimos que el gobierno de los Estados Unidos embargó efectivamente las asociaciones entre las empresas tecnológicas de los EE. UU. y el gigante móvil chino Huawei, debido a los temores sobre los estrechos vínculos entre Huawei y el estado chino.

Si se levantan más barreras como estas, fácilmente podría tener el efecto de prevenir la cooperación internacional en los desafíos tecnológicos y regulatorios de la ciberseguridad. Y eso solo es probable que beneficie a los malos.

3. Interferencia política más sofisticada

Las campañas de desinformación dirigidas a influir en la opinión pública casi se han convertido en una característica aceptada de la democracia en la actualidad. Ocurrió con las elecciones presidenciales de EE. UU. En 2021, parece seguro que volverán a aparecer en los titulares.

Hasta ahora, las elecciones dirigidas a delitos cibernéticos han tomado dos formas. El primero implica la difusión de «noticias falsas» y narrativas falsas, generalmente diseñadas para engañar a un candidato, a través de las redes sociales. El segundo son los ataques directos contra los candidatos o la infraestructura electoral digital.

Contrarrestar las narraciones falsas significa construir sistemas, ya sea automatizados o manuales, que pueden filtrar mentiras, propaganda y mala fe al analizar tanto el contenido como los metadatos, de dónde proviene la información y quién es probable que la haya creado.

Facebook y Google han invertido en tecnología diseñada para determinar si los mensajes políticos se ajustan o no a los patrones que sugieren que podría ser parte de una campaña específica de «noticias falsas». Esto ocurre por la enorme certeza de que estos métodos se están implantando cada vez más por los actores estatales con la finalidad de ocasionar revueltas políticas.

Se sospecha que el gobierno chino está tratando de impulsar una narrativa pro-China en torno a las elecciones en Taiwán y las protestas civiles en Hong Kong utilizando falsas cuentas de redes sociales.

Es probable que ambas formas de interferencia electoral digital se conviertan en un problema creciente en los próximos 12 meses, en parte debido al hecho de que han demostrado ser muy efectivas hasta ahora.

En consecuencia, podemos esperar una mayor inversión en tecnología diseñada para contrarrestarlos, así como esfuerzos para aumentar la conciencia pública sobre el tema.

4. Aumento de la brecha de habilidades de ciberseguridad

Durante 2021, la investigación sugiere que el número de trabajos de seguridad cibernética no cubiertos aumentará de solo 1 millón en 2014 a 3.5 millones. Es probable que este déficit de habilidades se convierta en un problema creciente de interés público durante la primera parte de esta nueva década.

Las amenazas que enfrentamos hoy en el ciberespacio, desde ladrones que intentan clonar identidades para llevar a cabo fraudes, hasta campañas de desinformación política diseñadas para alterar el curso de las democracias, solo se harán más intensas a menos que haya suficientes personas con las habilidades para contrarrestarlas.

Sin invertir en capacitar al personal existente sobre cómo prevenir o mitigar los ataques cibernéticos en su campo, ni contratar expertos con las habilidades para detectar nuevas amenazas en el horizonte, la industria puede perder cientos de millones de dólares.

El coste promedio actual incurrido por una empresa que sufre una violación de datos es de unos 9 millones de euros. Entre las organizaciones que han implementado defensas de ciberseguridad totalmente automatizadas, ese coste cae a 3 millones.

Por supuesto, la implementación de estas defensas maduras requiere acceso a una fuerza laboral de ciberseguridad capacitada y experimentada, algo que es probable que se convierta cada vez más en un desafío en los próximos años.

5. Aumento del pirateo de datos y robo de vehículos

Incluso antes de entrar en el tema de los automóviles sin conductor, los vehículos de hoy son básicamente fábricas de datos móviles. Los automóviles modernos están equipados con una variedad de dispositivos GPS, sensores y plataformas de comunicación y entretenimiento en el automóvil que los convierten en un objetivo cada vez más rentable para piratas informáticos y ladrones de datos.

Los delincuentes han aprendido a aprovechar las redes privadas a través de electrodomésticos y dispositivos inteligentes conectados, gracias a la falta de estándares de seguridad entre los miles de fabricantes de dispositivos y proveedores de servicios.

Del mismo modo, es probable que el automóvil se convierta cada vez más en la puerta de atrás elegida en los próximos años gracias a la creciente cantidad de datos que recopilan y almacenan sobre nuestra vida cotidiana. Los atacantes tendrán la opción de apuntar a los propios vehículos, tal vez usarlos para acceder a cuentas de correo electrónico y luego a información personal. O los servicios en la nube donde nuestros datos se envían rutinariamente para almacenamiento y análisis.

La recolección y reventa a gran escala de estos datos en el mercado negro es muy lucrativa para los cibercriminales.

Otro riesgo muy real es que los atacantes pueden llegar a entender los controles digitales y los requisitos de seguridad de los vehículos modernos.

La idea de secuestrar automóviles autónomos y asumir sus controles puede parecer descabellada en este momento, pero es una amenaza que la industria automotriz y los legisladores están tomando en serio. Durante 2021, es probable que veamos más debate sobre este aspecto de la seguridad de los vehículos autónomos, ya que el marco regulatorio que les permitirá operar en nuestras carreteras continúa tomando forma.

6. Vulnerabilidad de los sistemas ICS / SCADA

En 2021, el número de ataques cibernéticos contra ICS / SCADA en infraestructuras críticas continuará creciendo. En la mayoría de los casos, estos sistemas no fueron diseñados para ser expuestos en línea o controlados de forma remota. Por esta razón, será bastante fácil para los atacantes explotar las vulnerabilidades que los afectan.

La mayoría de los ataques efectuados por ciberdelincuentes contra los sistemas ICS / SCADA son de carácter oportunista. Sin embargo, es posible que los hackers patrocinados por el Estado realicen ataques dirigidos contra la infraestructura crítica de estados extranjeros.

Las industrias de energía, salud e instalaciones serán los sectores más focalizados en el próximo año.

La buena noticia es que los proveedores de soluciones ICS lanzarán nuevos productos que implementarán controles de seguridad eficientes. Sin embargo, las organizaciones tardarán años en reemplazar las tecnologías heredadas que utilizan.

7. Crecimiento de ataques a la cadena de suministro

Los ataques a la cadena de suministro de software y hardware caracterizarán el panorama de amenazas en los próximos 12 meses. Los atacantes intentarán comprometer la cadena de suministro de paquetes de software legítimos mediante la implantación de malware.

Los ataques tendrán como objetivo tanto a los proveedores de software durante la fase de desarrollo como a terceros. Los atacantes buscan reemplazar el software legítimo y las actualizaciones relacionadas con versiones contaminadas para distribuir malware a través del canal de distribución del software legítimo.

Los ataques a la cadena de suministro de software aumentarán en volumen y nivel de sofisticación. Y no podemos subestimar el riesgo de ataques de cadena de suministro de hardware más insidiosos.

En los últimos meses, los actores de amenazas desarrollaron rootkits maliciosos para comprometer UEFI / BIOS. La probabilidad de que un malware como este pueda comprometer la cadena de suministro de software enviado a millones de ordenadores es alta.

Dichos ataques son muy difíciles de detectar y el malware implantado sería muy difícil de eliminar, incluso después de reformatear los ordenadores.

Los ataques a la cadena de suministro serán una opción de ataque privilegiada para los actores de los estados nacionales que exploran métodos nuevos y más sofisticados para infiltrarse en las organizaciones objetivo.

8. Aumento de las amenazas de la red 5G

Con el despegue de la tecnología 5G el año pasado, muchas élites de la industria esperan que las redes 5G comiencen a ser más frecuentes en 2021. ¿Qué significa esto?

Primero, su alta velocidad podría revolucionar la experiencia en línea para los usuarios de Internet en todas partes. Pero según un informe de la Unión Europea, también podría hacer que las redes sean más vulnerables a los cibercriminales.

Con el aumento de las maneras en las que los atacantes pueden acceder a datos confidenciales, y el incremento de los desafíos como la monitorización de riesgos en dispositivos sin un enrutador Wi-Fi, las personas deberán ser proactivas a medida que desarrollen nuevas soluciones de seguridad.

Mejores prácticas para ciberdefensa y protección

Es fácil sentirse frustrado por la gravedad del entorno de amenaza. Sin embargo, es posible proteger su negocio de las amenazas cibernéticas. Los consumidores también pueden defenderse.

Defensa cibernética para empresas

Las mejores prácticas empresariales para la defensa de la defensa cibernética incluyen contramedidas básicas pero extremadamente importantes como los sistemas de parches. Cuando un proveedor de tecnología descubre (o se le informa) un fallo de seguridad en su producto, generalmente escribe un código que corrige o «repara» el problema.

Por ejemplo, si Microsoft descubre que un pirata informático puede obtener acceso de root a Windows Server a través de una explotación de código, la compañía emitirá un parche y lo distribuirá a todos los propietarios de licencias de Windows Server. Ellos, entre muchos otros, hacen esto al menos una vez al mes.

Muchos ataques fallarían si los departamentos de TI aplicaran todos los parches de seguridad de manera oportuna.

Están llegando al mercado una gran cantidad de nuevas tecnologías y servicios que hacen que sea más fácil montar una defensa sólida contra las amenazas cibernéticas.

Éstos incluyen:

Servicios de seguridad tercerizados

Sistemas que permiten la colaboración entre los miembros del equipo de seguridad.

Herramientas de simulación de ataque continuo

Soluciones puntuales para anti-phishing y navegación segura

Defensa cibernética para individuos

Para las personas, las mejores prácticas son simples. La buena noticia es que, en la mayoría de los casos, algunas organizaciones de seguridad bastante grandes se interponen entre el consumidor y el hacker.

Todavía hay medidas preventivas que debe tomar para ayudar a garantizar la seguridad de su información:

Contraseña de higiene. Las grandes organizaciones de seguridad no pueden proteger a los consumidores contra el phishing o los piratas informáticos que pueden adivinar contraseñas como «1234.» El sentido común y la seguridad de las contraseñas pueden recorrer un largo camino para proteger a los consumidores de las amenazas cibernéticas.

Software antivirus. Utiliza software antivirus y mantén su sistema actualizado con escaneos programados y automatizados.

Precaución contra los ataques de phishing. Ten cuidado al abrir archivos adjuntos. Phishing y correos electrónicos de spear phishing que parecen reales pero no lo son. Por ejemplo, si recibes un correo electrónico que dice «factura vencida» con un archivo adjunto en PDF, no lo abras a menos que estés 100% seguro de saber quién lo envió. Si lo verifica bien, probablemente verás que proviene de un correo electrónico inusual.

Podemos encontrarnos en un momento horrible para las empresas y los consumidores que se preocupan por los riesgos cibernéticos. Las amenazas ciertamente existen, y se están volviendo cada vez más potentes y frecuentes. Los atacantes son variados, con muchos desequilibrios preocupantes entre los atacantes y sus objetivos.

Pero no tengas miedo.

Incluso si una empresa es objetivo de un poderoso estado-nación, aún es posible proteger activos digitales críticos. Se necesita planificación y compromiso de recursos. Pero un buen equipo de operaciones de seguridad o una persona proactiva pueden estar al tanto de la mayoría de las amenazas cibernéticas más graves.